



## **KAJE Fin Services LTD.**

### **ANTI-MONEY LAUNDERING & TERRORIST FINANCING MANUAL**

#### **1. GENERAL DEFINITIONS**

For the purposes of this Manual, unless the context shall prescribe otherwise:

1.1. “Act” means The FATF Recommendations, the international anti-money laundering and combatting the financing of terrorism and proliferation (AML/CFT) standards, and the FATF Methodology to assess the effectiveness of AML/CFT systems. as amended from time to time;

1.2. “Account” means any facility or arrangement in which a reporting entity does any of the following:

1.2.1. accepts deposits of funds;

1.2.2. allows withdrawals of funds;

1.2.3. pays negotiable or transferable instruments or cheques or payment orders drawn on behalf of any person, or collects negotiable or transferable instruments or cheques or payment orders on behalf of a person, and includes any facility or arrangement for a safety deposit box or for any other form of safe deposit or held in a cash management trust;

1.3. “Activity” means a series of transactions or an act or omission of an act;

1.4. “Assisting Entity” means:

1.4.1. a law enforcement agency or supervisory body outside Marshall Islands or any other institution or agency of the relevant foreign state; or

1.4.2. an international organization established by the governments of foreign states; or

1.4.3. a body outside Marshall Islands with functions similar to the Unit; or

1.4.4. a law enforcement agency or supervisory body within Marshall Islands;

1.5. “AML” means Anti-Money Laundering “Beneficial Owner” means:

1.5.1. a natural person who ultimately owns or controls the right to or benefits from a fund; or

1.5.2. a person who exercises ultimate effective control over a legal person or legal arrangement;

1.6. “Beneficiary” has same meaning as beneficial owner

1.7. “Board of Directors” means the board of directors of the Company;

1.8. “Business Relationship” means a business, professional or commercial relationship which is:

1.8.1. connected with the professional activities of the reporting entity and

1.8.2. which is expected, at the time when the contact was established, to have an element of duration.

1.9. “Cash” means any coin or paper money that is designated as legal tender in the country of issue; 5

1.10. “CTF” means Counter-Terrorism Financing

1.11. “Currency” includes:

1.11.1. the cash of Marshall Islands or of a foreign country that is designated as legal tender and which is customarily used and accepted as a medium of exchange in the country of issue; or

1.11.2. monetary instruments that may be exchanged for money, including cheques, travelers cheques, money orders and negotiable instruments in a form in which title passes on delivery; or

1.11.3. a precious metal or precious stone; or

1.11.4. such other monetary instruments specified by the Minister by Order; or

1.11.5. currency in electronic form including debit cards, credit cards, pre-paid mobile phones and any other electronic device with a stored value;

1.12. “Customer” in relation to a transaction, business relationship or an account includes:

1.12.1. the person in whose name or for whom a transaction, relationship or account is arranged, opened or undertaken; or

1.12.2. a signatory to the transaction, relationship or account; or

1.12.3. any person to whom, a relationship or an account or rights or obligations under a transaction or relationship have been assigned or transferred;

1.12.3. or any person who is authorised to conduct the transaction or control the relationship or account; or

1.12.4. such other persons prescribed for the purposes of this definition

1.13. “Company” means KAJE FIN SERVICES LTD which is incorporated in the Republic of Marshall Islands with registration number 83226.

1.14. “Data” means representations, in any form, of information or concepts;

1.15. “Director” means the Director of the Financial Intelligence Unit appointed under section 7 of the Act; “director of a person or entity” means:

1.15.1. (any person occupying the position of a director of the person or entity, regardless of the name given to the position; or

1.15.2. any person held out by the person or entity to be a director;

1.16. “Financing of terrorism offence means an offence against section 6 of the Counter Terrorism and Transnational Organised Crime Act [CAP 313] as amended from time to time;

1.17. “Fund” includes:

1.17.1. currency; or

1.17.2. assets of any kind, whether corporeal or incorporeal, moveable or immovable, tangible or intangible; or

1.17.3. legal documents or instruments in any form including electronic or digital, evidencing title to, or interest in, such assets, including but not limited to bank credits, traveller’s cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit; or

1.17.4. any legal or equitable interest in any such asset

1.18. “Law Enforcement Agency” means:

1.18.1. the Marshall Islands Police Force; or

1.18.2. the Department of Customs and Inland Revenue; or

1.18.3. the Department of Immigration; or

1.18.4. a Police organisation or institution outside of Marshall Islands; or

1.18.5. an organisation responsible for criminal prosecutions or investigation inside or outside of Marshall Islands; or

1.18.6. such other persons prescribed for the purposes of this definition;

1.19. “Minister” means the Prime Minister

1.20. “Money laundering entity” means a person or group prescribed under subsection 53(2) of the Act as amended from time to time;

1.21. “Money laundering offence” means an offence against section 11 of the Proceeds of Crime Act [CAP 284]; as amended from time to time;

1.21.1. “ML” means Money Laundering

1.22. “Originator” means the account holder or where there is no account, the person that places the order with a reporting entity to perform an electronic funds transfer;

1.23. “Owner of a person or entity” means a person who has a legal entitlement of 25% or more of the person or entity by way of ownership of shares or otherwise, and own and ownership have a corresponding meaning;

1.24. “Person” means any natural or legal person and includes any statutory body, company or association or body of persons corporate or unincorporated;

1.25. “Politically Exposed Person” means an individual who is or has been entrusted with prominent public functions such as the Head of State, the Prime Minister, Ministers, senior politicians, senior Government officials, judicial or military officials, senior executive members of state owned corporations or international organisations and officials of a political party;

1.26. “Prescribed entity” means:

1.26.1. a specified entity within the meaning of the Counter Terrorism and Transnational Organised Crime Act [CAP 313] as amended from time to time; or

1.26.2. a money laundering entity; or

1.26.3. a person or group that has been designated by the Security Council of the United Nations, acting under Resolutions of the Security Council relating to terrorism,

to be a person or entity associated with the Taliban or an Al Qaida terrorist group.

1.25. "Prescribed Person"

1.25.1. For the purpose of paragraph (e) of the definition of customer under section 1 of the Act as amended from time to time and as described above, the following persons are prescribed as customer:

1.25.2. in the case of a Charitable Association, a Credit Union or a Cooperative Society -the person who provide funds to these entities;

1.25.3. in the case of a Real Estate Agent, a Motor Vehicle Dealer, a Property Dealer under paragraph 2(r)(xii) of the Act as amended from time to time or a Lawyer, Accountant or Notary under paragraph 2(o) of the Act as amended from time to time -the purchaser and/or vendor of properties.

1.26. For the purpose of paragraph (f) of the definition of law enforcement agency under section 1, of the Act as amended from time to time, law enforcement agency also includes a person appointed by a competent authority under relevant laws of Marshall Islands to:

1.26.1. collect information on; or

1.26.2. inspect; or

1.26.3. investigate; or

1.26.4. prosecute,

an offence under the laws of Marshall Islands or laws of another country, if that offence is also an offence under the laws of Marshall Islands."

1.27. "Prescribed threshold for large cash transaction"

For the purpose of section 27 of the Act as amended from time to time, the prescribed threshold for large cash transaction is 100,000\$ or its equivalent in foreign currency.

1.27.1. If a person:

1.28. "Proliferation Financing" means the act of providing funds or financial service, which are used or will be used, in whole or in part:

1.28.1. for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling of weapons; or

1.28.2. for the use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use good used for

non- legitimate purposes), that contravenes any laws of Marshall Islands."

1.29. "Record" means any material on which information is recorded or marked and which is capable of being read or understood by a person, computer system or other device;

1.30. "Reporting entity" has the meaning given by section 2 of the Act as amended from time to time.

1.31. "Supervisory Body" means:

1.32. the RMI Banking Commission of Marshall Islands; or

1.33. the registrar of Cooperatives; or

1.34. a body outside Marshall Islands with functions similar to the RMI Banking Commission of Marshall Islands; or such other persons prescribed for the purposes of this definition;

1.35. "Suspicious Activity Report" means a report prepared under Part 6 of the Act as amended from time to time;

1.36. "Suspicious Transaction Report" means a report prepared under Part 6 of the Act as amended from time to time;

1.37. "Terrorist Organization" includes an individual or organization prescribed by the Regulations to be a terrorist organization;

1.38. "Transaction" means:

1.39.1. any deposit, withdrawal, exchange or transfer of fund whether:

1.39.1.1. in cash; or

1.39.1.2. by cheque, payment order or other instrument; or

1.39.1.3. by electronic or other non-physical means; or

1.39.1.4. in satisfaction, whether in whole or part, of any contractual or other legal obligation.

1.39.2. Without limiting subsection (1), a transaction includes the following:

1.39.2.1. the establishment and maintenance of a business relationship; or

1.39.2.2. the opening and maintenance of an account; or

1.39.2.3. the engagement of a service; or

1.39.2.4. any payment made in respect of a lottery, bet or other game of chance; or

1.39.2.5. the establishment, creation or maintenance of a legal person or legal arrangement; or

1.39.2.6. such other transactions as may be prescribed.  
“TF” means and Terrorism Financing.

1.40. “Unit” means the Financial Intelligence Unit

## **2. INTRODUCTION**

2.1. The purpose of the Manual is to lay down the Company’s internal practice, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing. The Manual is developed and periodically updated by the Money Laundering Compliance Officer (hereinafter the “MLCO”) based on the general principles set up by the Company’s Board of Directors (hereinafter the “Board”) in relation to the prevention of Money Laundering and Terrorist Financing. All amendments and/or changes of the Manual must be approved by the Board. The Manual is applicable and shall be communicated by the MCLO to all the employees and business units of the Company that manage, monitor or control in any way the Clients’ transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein as well as to appointed introducers and other partners and related parties of the Company. Any questions regarding the Manual should be addressed to the MLCO.

2.2. The Manual has been prepared to comply with the provisions of the respective The FATF Recommendations, the international anti-money laundering and combatting the financing of terrorism and proliferation (AML/CFT) standards, and the FATF Methodology to assess the effectiveness of AML/CFT systems and as these are amended from time to time. When Company’s personnel becomes aware of breaches of law, internal and or external regulations including this Manual, in relation to Money Launder and Terrorist Financing they should immediately bring this to the attention of the MLCO.

## **3. MANUAL APPLICABILITY: TRADING IN CFDs AND OTHER DERIVATIVE FINANCIAL INSTRUMENTS**

3.1. The Manual applies to all various types of services offered to the Company’s Clients as well as the relevant Company’s dealings with its Clients, including trading transactions in CFDs and other derivative financial

instruments, which either do not aim to physically deliver the agreed foreign currency or are not materially settled in cash (foreign exchange spot trading), irrespective of the Client account size and frequency of trading. In this respect, the MLCO shall be responsible to update the Manual so as to comply with Republic Of The Marshall Islands The Registrar Of Corporations’s future requirements, as applicable, regarding the Client identification and due diligence procedures which a CIF must follow, for Clients who deal in foreign exchange trading transactions in CFDs and other derivative financial instruments with the Company.

## **4. AML/CFT COMPLIANCE OFFICER**

### **4.1. General**

4.1. The AML/CFT Compliance Officer (hereafter “the Compliance Officer”) shall belong hierarchically to higher ranks of the Company’s organisational structure (i.e. management of the Company) so as to command the necessary authority. The Compliance Officer shall be a high ranking Company officer (i.e. senior officer) either on a full time or part time basis, who is skilled, knowledgeable and experienced in the financial services or other business activities, as applicable. Furthermore, the Compliance Officer leads the Company’s Money Laundering Compliance procedures and processes and report to the Senior Management. The Compliance Officer shall also have the resources, expertise as well as access to all relevant information necessary to perform his duties adequately and efficiently. Where it is deemed necessary due to the volume and/or the geographic spread of the services/activities, assistants of the compliance officer are appointed, by geographical district or otherwise for the purpose of assisting the compliance officer and passing internal suspicion reports to him. The Company communicates in writing immediately to the Director, of its Compliance Officer’s appointment or any change of appointment or termination of appointment.

### **4.2. Duties of Compliance Officer**

The duties of the Compliance Officer shall include, inter alia, the following:

4.2.1. responsible for ensuring compliance with the requirements Act and Regulations

4.2.2. responsible for reporting suspicious transactions and activities to the Republic Of The Marshall Islands The Registrar Of Corporations

4.2.3. report financial transactions exceeding the prescribed threshold to the Republic Of The Marshall Islands The Registrar Of Corporations;

4.2.4. design the Company's AML Manual, implement effective policies, processes and procedures for customer due diligence, record keeping, transaction monitoring, transaction reporting and reporting suspicious transactions and activities in line with the Act as amended from time to time.

4.2.5. to receive information from the Company's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. The information is received in a written report form, namely the Internal Suspicion Report (ISR) (Appendix 7 of the Manual);

4.2.6. to evaluate and examine the information received as per point (e) above, by reference to other relevant information and discuss the circumstances of the case with the informer and where appropriate, with the informer's superiors. The evaluation of the information of point (e) above shall be done on a report namely Internal Evaluation Report (IER), (Appendix 8 of the Manual);

4.2.7. if following the evaluation described in point (f) above, the Compliance Officer decides not to notify the Director (Republic Of The Marshall Islands The Registrar Of Corporations) then he should fully explain the reasons for such a decision on the Internal Evaluation Report;

4.2.8. to monitor and assess the correct and effective implementation of the policies, the practices, measures, procedures and controls of point (a) above and in general the implementation of the Manual. In this respect, the Compliance Officer shall apply appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him with all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. In the event that the Compliance Officer identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls,

gives appropriate guidance for corrective measures and where deems necessary informs the Board;

4.2.9. to provide advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing;

4.2.10. to acquire the knowledge and skills required for the improvement of the appropriate procedures for recognising, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing as applicable and relevant to the services being offered by the Company;

4.2.11. to determine whether the Company's departments and employees need further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organises appropriate training sessions/seminars. In this respect, the Compliance Officer prepares and applies an annual staff training program. Further, the Compliance Officer assesses the adequacy of the education and training provided.

4.2.12. keep a register of all reports made to the Republic Of The Marshall Islands The Registrar Of Corporations and all reports made internally to them by employees.

4.2.13. Preparation and submission to the Director of the annual AML and CFT Compliance Report pursuant to section 31 of the Act as amended from time to time

4.2.14. Preparation and submission of ML&TF Risk Assessment Report pursuant to section 35 of the Act as amended from time to time if the Director requests the Company to do so.

## **5. OBLIGATIONS OF AUDITORS**

5.1. The Company's Auditors must report an STR (Appendix 3) if they have reasonable grounds to suspect that a transaction or attempted transaction, or information that they have in their possession involves proceeds of crime or is related to terrorist financing. The report must be submitted to the Director as soon as possible, but no later than 2 working days after forming the suspicion. Failure to comply without reasonable grounds, the Auditors commit an offence and are liable on conviction. The reports must be sent to the Director by way of fax or electronic mail or hand delivery. A report may be given orally including by telephone. In the case of oral report, a written report (STR or SAR) must be prepared and

submitted to the Director within 24 hours from the oral report has been given. Failure to comply with the above, is an offence and the Auditors are liable on conviction. Internal audit plays an important role in independently evaluating the risk management and controls, through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. External auditors also have an important role to play in monitoring the Company's internal controls and procedures, and in confirming that they are in compliance with the requirements of the AML&CTF Act. Entities must ensure that their internal controls and procedures are assessed by external and independent auditors on a regular basis.

## **6. REPORTING REQUIREMENTS**

### **6.1. ML and CFT Compliance Report**

The AML and CFT Compliance Report of the Compliance Officer is a significant tool for assessing the Company's level of compliance with its obligation laid down in the applicable Act and Regulations as amended.

6.2. The Compliance Officer's Annual Report must be:

6.2.1. made in the prescribed form (refer to Appendix 1 of this Manual); and

6.2.2. sent/lodged to the Director within a prescribed time frame.

6.3. Failure to comply with the points above, the reporting entity commits an offence and is liable on conviction. The Director may request any further information from a reporting entity if the reporting entity has made a report on a transaction, attempted transaction, activity or attempted activity or has provided information under Part 7 of the Act to the Director. A reporting entity who fails without reasonable grounds to comply with the latter commits an offence and is liable on conviction.

### **6.4. ML&TF Risk Assessment Report**

The Director may by notice in writing, require a reporting entity to:

- (a) carry out a money laundering and terrorism financing risk assessment; and
- (b) prepare a written report setting out the results of the assessment; and
- (c) provide a copy of the report within the period specified in the notice to the Director.

It is important to note that the ML&TF Assessment Report is applicable and mandatory only when and if the Director requests for it. The report must be in the prescribed form (refer to Appendix 2 of the Manual). Failure to comply without any notice, a reporting entity commits an offence and is liable on conviction.

### **6.3. Suspicious Transaction Report (STR)**

The Company through its Compliance Officer must make a report (refer to Appendix 3 of the Manual) of the transaction or attempted transaction to the Director not later than 2 working days if the reporting entity suspects or has reasonable grounds to suspect that a transaction or attempted transaction involves proceeds of crime or is related to terrorist financing. The Company must not proceed any further with the transaction unless directed to do so by the Director. Failure to comply, is an offence and the Company is liable on conviction.

### **6.4. Suspicious Activity Report (SAR)**

The Company through its Compliance Officer must make a report (refer to Appendix 4 of the Manual) of the activity or attempted activity to the Director not later than 2 working days if a reporting entity suspects or has reasonable grounds to suspect that an activity or attempted activity involves proceeds of crime or is related to terrorist financing. The Company must not proceed any further with the activity unless directed to do so by the Director. Failure to comply, is an offence and the Company is liable on conviction.

### **6.5. Transaction Conducted By Money Laundering Entities**

The Company through its Compliance Officer must report an STR (Appendix 3) if a money laundering entity conducts or seeks to conduct a transaction through or by using the Company and such transaction is deemed to be a suspicious transaction involving proceeds of crime. The report must be submitted to the Director as soon as possible, but no later than 2 working days after forming the suspicion. Further, the Company must not proceed any further with the transaction unless directed do so by the Director. Failure to comply, is an offence and the Company is liable on conviction.

### **6.6. Transaction Involving Terrorist Property**

The Company through its Compliance Officer must report an STR (Appendix 3) if it has information in its

possession concerning any transaction or attempted transaction which it suspect to involve terrorist property, property linked to terrorist or terrorist organisation. The report must be submitted to the Director as soon as possible, but no later than 2 working days after forming the suspicion. Further, the Company must not proceed any further with the transaction unless directed do so by the Director. Failure to comply, is an offence and the Company is liable on conviction.

#### 6.7. Certain Transaction with no Legitimate Purpose

The Company through its Compliance Officer must report an STR (Appendix 3) if there is suspicion that a transaction or attempted transaction:

- (a) is complex, unusual or large and does not have any apparent or visible economic or lawful purpose; or
- (b) is part of an unusual pattern of transactions that does not have any apparent or visible economic or lawful purpose.

The report must be submitted to the Director as soon as possible, but no later than 2 working days after forming the suspicion. Further, the Company must not proceed any further with the transaction unless directed do so by the Director. Failure to comply, is an offence and the Company is liable on conviction.

#### 6.8. Method of Submission

The reports specified in sections above, must be sent to the Director by way of fax or electronic mail or hand delivery. A report may be given orally including by telephone. In the case of oral report, a written report (STR or SAR) must be prepared and submitted to the Director within 24 hours from the oral report been given. Failure to comply with the above, is an offence and the Company is liable on conviction.

#### 6.9. Report of Large Cash Transaction

The Company must make a report (Appendix 5 of Manual) to the Director on a transaction of an amount of cash that exceeds the prescribed threshold or its equivalent in foreign currency, whether the transaction is conducted as a single transaction or two or more transactions that appear to be linked. A reporting of large cash transaction must be made and submitted to the Director within the following time frame:

(a) In the case of transaction or transfer in Marshall Islands, within 10 working days after the transaction or transfer is made; and

(b) In the case of transaction or transfer in a foreign currency, within 2 working days after the transaction or transfer is made.

Failure to comply with the above, is an offence and the Company is liable on conviction. If the Company conducts the transactions for the sole or dominant purpose of ensuring or attempting to ensure that a report in relation to such transactions is not made, then it commits an offence and is liable on conviction as described above.

#### 6.10. Report of International Currency Transfers

The Company must make a report (Appendix 6 of Manual) to the Director:

(a) on any electronic transmission of currency or other currency transfer out of Marshall Islands that exceeds the prescribed threshold or its equivalent to foreign currency in the course of a transaction, whether conducted as a single transaction or by way of two or more transactions that appear to be linked; or

(b) on any electronic receipt of currency or other currency receipts from outside Marshall Islands that exceeds the prescribed threshold or its equivalent to foreign currency in the course of a transaction, whether conducted as a single transaction or by way of two or more transactions that appear to be linked or

(c) if the Company uses a service of a third party to receive or transmit electronic transaction or other currency transfer that exceeds the prescribed threshold or its equivalent to foreign currency in the course of a transaction, whether conducted as a single transaction or by way of two or more transactions that appear to be linked.

Failure to comply with the above, is an offence and the Company is liable on conviction. If the Company conducts the transactions for the sole or dominant purpose of ensuring or attempting to ensure that a report in relation to such transactions is not made, then it commits an offence and is liable on conviction as described above.

#### 6.11. Obligation to Submit Additional Information

The Director may request any further information from the Company if the Company has made a report on a transaction, attempted transaction, activity or attempted

activity or has provided information under this section to the Director. Failure to comply with the above without reasonable grounds, is an offence and the Company is liable on conviction.

#### 6.12. Prohibition of Tipping Off/Alerting Clients

Directors, officers and employees, agents and contractors of reporting entities are prohibited from disclosing the fact to the client that an STR, SAR or related information is being reported to the Republic Of The Marshall Islands The Registrar Of Corporations. In case the Company forms a suspicion that transactions relate to proceeds of crime or terrorist financing, it should take into account the risk of tipping off when performing the client due diligence (CDD) process. If the Company reasonably believes that performing the CDD process will tip-off the client or potential client, it may choose not to pursue that process, and should file an STR or SAR. The Company should ensure and take measures so that its employees, staff and agents are aware of and are sensitive to these issues when conducting CDD.

## 7. RECORD-KEEPING PROCEDURES

### 7.1. General

The Company and in particular the Compliance Officer must keep records of all transactions in such a manner as to enable the transactions to be readily reconstructed at any time by the Director to the extent that it is available, without undue delay. In line with the requirements outlined in the AML&CTF ACT and the AML&CTF Regulation, the Company shall maintain records including but not limited, of the following:

#### 7.1. Transaction:

- its transactions and related documentation;
- the nature of the transaction;
- the amount of the transactions and the currency in which it was denominated;
- the date on which the transaction was conducted;
- the name, address and occupation, business or principal activity of the person conducting the transaction and person for whom the transaction is conducted and for whose ultimate benefit the transaction is being conducted;
- the type and identifying number of any account/service with the entity involved in the transaction;

- if the transaction involves a negotiator instrument, the names of the drawer, the drawing institution, the payee and the amount and date of instrument and detail of endorsement;

- the name and address of the entity, and of each officer, employee or agent who prepared the relevant record;

- account files, business correspondence and findings of CDD analysis relating to the transaction;

- any other information relating to the transaction.

In relation to the transaction, the records must be kept for a minimum period of 6 years from the date on which the transaction was made and in such a manner as to enable the transactions to be readily reconstructed at any time by the Director. Further to this, the said records must contain the prescribed information as defined in this Manual.

#### 7.2. Identification- Verification:

- If evidence of a customer's identity and verification is obtained under the CDD processes, the Company must maintain a record that indicates the kind of evidence that was obtained and either a copy of the evidence or information that enable a copy of it to be obtained. The records must be kept for a minimum of 6 years after the closure or termination of the account, service or business relationship.

#### 7.3. Reports made to Director:

- a record of any suspicious transaction, suspicious activity or other report made to the Director as per section 8 of this Manual

- a record of any enquiry relating to money laundering or the financing of terrorism made to the Director; and

- a record of a finding referred to under subsection 18(2) of the Act as amended from time to time which relates to documentation and information obtained in relation to intermediaries or third party introducers

A reporting entity must keep records of the reports mentioned in this section for a period of 6 years after the date on which the report or the enquiry was made.

#### 7.4. AML and CFT Manual:

- a record of the adoption of an AML and CFT Procedure Manual; and

- retain the AML and CFT Procedure Manual for a period of 12 months.

In all of the above cases mentioned in this section should the Company fails to meet the above mentioned requirement of keeping records, commits an offence and is liable on conviction.

## **8. EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING**

### **8.1. Employees' Obligations**

(a) The Company's employees shall be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing.

(b) The employees must cooperate and report to the Compliance Officer, without delay, anything that comes to their attention in relation to transactions or any activity in a Client's accounts for which there is a slight suspicion that are related to money laundering or terrorist financing.

(c) The Company's employees shall fulfil their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after they submit the Internal Suspicion Report (Appendix 7 of Manual) to the Compliance Officer

### **8.2. Employee's Education and Training Policy**

The Compliance Officer shall ensure by introducing a complete employee's education and training program that all employees are fully aware of their legal obligations according to inter alia:

(a) The systems and procedures in accordance to this Manual and/or group-wide procedure manual;

(b) The AML/CTFT Act and the relevant AML//CFT Regulations as amended from time to time;

The timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Company. The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the financial system. The training program aims at educating the Company's employees on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose. The training program will have a different structure for new employees, existing employees and for different departments of the Company according to the services that they provide. On-going training shall be given at

regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments. Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the entity itself. Some form of high- level general awareness training is therefore suggested for those staff that may not be involved in dealing with customers on a day-to-day basis.

The Compliance Officer provides advice and guidance to the employees of the Company on subjects related to Money Laundering and Terrorist Financing.

### **8.3. Compliance Officer's Education and Training Program**

The Senior Management of the Company shall be responsible for the Compliance Officer to attend external training. Based on his/her training, the MLCO will then provide training to the employees of the Company. The main purpose of the Compliance Officer's training is to ensure that relevant employee(s) become aware of inter alia:

- the AML/CFT Act and the AML/CFT Regulations as amended from time to time
- the Company's Anti-Money Laundering Policy and Procedures
- the statutory obligations of the Company to report suspicious transactions
- the employees own personal obligation to refrain from activity that would result in money laundering
- the importance of the Clients' due diligence and identification measures requirements for money laundering prevention purposes.

## **9. RISK-BASED APPROACH**

### **9.1. General Policy**

The Company shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of Money Laundering and Terrorist Financing appears to be comparatively higher.

Further, the MLCO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of the Manual.

## 9.2. Risk-Based Approach Adopted

The adopted risk-based approach that is followed by the Company, and described in the Manual, has the following general characteristics:

- recognises that the money laundering or terrorist financing threat varies across Clients, countries, services and financial instruments
- allows the Board to differentiate between Clients of the Company in a way that matches the risk of their particular business
- allows the Board to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics
- helps to produce a more cost-effective system
- promotes the prioritization of effort and actions of the Company in response to the likelihood of Money Laundering and Terrorist Financing occurring through the use of the Investment and Ancillary Services provided by the Company.

9.2.1. Specific Measures: The risk-based approach adopted by the Company, and described in the Manual, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the Money Laundering and Terrorist Financing risks faced by the Company.

Such measures include:

- identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, financial instruments, services, and geographical areas of operation of its Clients;
- Documenting (e.g. the present Manual) the policies, measures, procedures and controls to ensure their uniform application across the Company by persons specifically appointed for that purpose by the board of directors;
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
- continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

The application of appropriate measures and the nature and extent of the procedures on a risk-based approach depends on different indicators.

Such indicators include the following:

- the scale and complexity of the services offered
- geographical spread of the services and Clients
- the nature (e.g. non face-to-face) and economic profile of Clients as well as of financial instruments and services offered
- the distribution channels and practices of providing services
- the volume and size of transactions
- the degree of risk associated with each area of services
- the country of origin and destination of Clients' funds
- deviations from the anticipated level of transactions
- the nature of business transactions.

The MLCO shall be responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the MLCO shall also be responsible for the adequate implementation of the policies, procedures and controls on a risk-based approach. The Auditors shall be responsible for reviewing the adequate implementation of a risk-based approach by the MLCO, at least annually.

## 9.3. Identification of Risks

### 9.3.1. General Principles

The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed. The MLCO has the responsibility to identify, record and evaluate all potential risks of money laundering and terrorist financing. The Company shall assess and evaluate the risks it faces, for the use of the Investment and Ancillary Services for the purpose of Money Laundering or Terrorist Financing. The particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk.

### 9.3.2. Company Risks

The following, inter alia, are sources of risks which the Company faces with respect to Money Laundering and Terrorist Financing:

#### 9.3.2.1 Risks based on the Client's nature:

- complexity of ownership structure of legal persons
- companies with bearer shares
- companies incorporated in offshore centres
- PEPs
- Clients engaged in transactions which involves significant amounts of cash
- Clients from high risk countries or countries known for high level of corruption or organised crime or drug trafficking
- unwillingness of Client to provide information on the Beneficial Owners of a legal person.

#### 9.3.2.2. Risks based on the Client's behaviour:

- Client transactions where there is no apparent legal financial/commercial rationale
- situations where the origin of wealth and/or source of funds cannot be easily verified
- unwillingness of Clients to provide information on the Beneficial Owners of a legal person.

#### 9.3.2.3. Risks based on the Client's initial communication with the Company:

- non face-to-face Clients
- Clients introduced by a third person.

#### 9.3.2.4. Risks based on the Company's services and financial instruments:

- services that allow payments to third persons/parties
- large cash deposits or withdrawals
- products or transactions which may favour anonymity.

#### 9.4. Design and Implementation of Measures and Procedures to Manage and Mitigate the Risks

When the MLCO identifies (according to paragraphs 9.2. and 9.3.2 above) the risks the Company faces, then designs and implements the appropriate measures and procedures for the correct management and mitigation; especially of high risk clients.

Taking into consideration the assessed risks, the Company shall determine the type and extent of measures it will adopt in order to manage and mitigate the identified risks in a cost effective manner. These measures and procedures include:

- adaptation of the Client Due Diligence Procedures in respect of Clients in line with their assessed Money Laundering and Terrorist Financing risk
- requiring the quality and extent of required identification data for each type of Client to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence)
- obtaining additional data and information from the Clients, where this is appropriate for the proper and complete understanding of their activities and source of wealth and for the effective management of any increased risk emanating from the particular Business Relationship or the Occasional Transaction
- ongoing monitoring of high risk Clients' transactions and activities/activities, as and when applicable.

Determine the category of low risk customers and determine the category of high risk customers. In this respect, it is the duty of the MLCO to develop and constantly monitor and adjust the Company's policies and procedures with respect to the Client Acceptance Policy and Client Due Diligence and Identification Procedures of the Manual, respectively, as well as via a random sampling exercise as regards existing Clients.

#### 9.5. Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities change as well as the services and financial instruments provided by the Company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.

In this respect, it is the duty of the MLCO to undertake regular reviews of the characteristics of existing Clients, new Clients, services and financial instruments and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented, as applicable, and form part of the Annual Money Laundering Report.

### 10. CLIENT ACCEPTANCE POLICY

A clear Client Acceptance Policy (hereinafter the "CAP"), attached herein as Appendix 9 is developed and

established, which is completely in line with the provisions of the Act and the Regulations as amended from time to time. The CAP is prepared after detailed assessment of the risks faced by the Company from its customers and/or their transactions and/or their countries of origin or operations. The CAP, defines the criteria for accepting new Clients and defines the Client categorisation criteria which shall be followed by the Company and especially by the employees which shall be involved in the Client Account Opening process.

The MLCO shall be responsible for applying all the provisions of the CAP. In this respect, the Back Office Department together with the Sales and Support Department shall also be assisting the MLCO with the implementation of the CAP, as applicable.

#### 10.1. General Principles of CAP

The General Principles of the CAP are the following:

- (a) the Company shall classify Clients into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Client (i.e. Low Risk, Normal Risk and High Risk);
- (b) where the Client is a prospective Client, an account must be opened only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted, according to the principles and procedures set in Section 13 of the Manual;
- (c) all documents and data described in Section 13 of the Manual must be collected before accepting a new Client;
- (d) (no account shall be opened in anonymous or fictitious names(s);
- (e) no account shall be opened unless the prospective Client is approved by the MLCO or a person from the Company's compliance function

## 11. CLIENT IDENTIFICATION, KNOW YOUR CLIENT (KYC) AND DUE DILIGENCE PROCEDURES

The Company applies customer identification procedures, KYC and customer due diligence measures in the following cases:

- When establishing a business relationship;
- When carrying out occasional transactions that exceeds the prescribed threshold specified in the Act whether conducted as a single transaction or by way of two or more transactions that appear to be linked.
- When there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction;
- When there are doubts about the veracity or adequacy of previously customer identification data.

In this respect, it is the duty of the MLCO to apply all the relevant Client Identification Due Diligence Identification & KYC Procedures ("CDD & KYC") described in Appendix 10 of the Manual for the four (4) cases mentioned above. Furthermore, the compliance function shall also be responsible to collect and file the relevant Client identification documents, according to the recording keeping procedures described in the Manual. Further, the MLCO shall be responsible to maintain at all times and use during the application of Client due diligence and identification procedures template-checklists with respect to required documents and data from potential Clients, as per the requirements of the Act and the Regulations as amended from time to time.



## APPENDIX 1 - AML&CFT COMPLIANCE REPORT

Pursuant to The Republic of the Marshall Islands, Economic Substance Regulations, 2018 promulgated by the Registrar of Corporations responsible for non-resident domestic entities pursuant to the authority granted under section 129.5(2) of the Business Corporations Act, Part 1 of Title 52 of the Marshall Islands Revised Code entered into force on 1 January 2019 and have effect for financial periods commencing on or after 1 January 2019 the MLCO are required to complete and submit this report to the Director.

### INFORMER'S DETAILS

Name: ..... Tel: .....  
Department: ..... Fax: .....  
Position: .....

### CLIENT'S DETAILS

Name: .....  
Address: .....  
.....  
Date of Birth: ..... Tel: .....  
Occupation: ..... Fax: .....  
Details of Employer: .....  
Passport No.: ..... Nationality: .....  
ID Card No.: .....  
Other ID Details: .....

### INFORMATION/SUSPICION

Brief description of activities/transaction: .....  
.....  
.....  
.....  
.....  
Reason(s) for suspicion: .....  
.....  
.....  
.....  
.....

Informer's Signature Date .....

### FOR MLCO USE

Date Received: ..... Time Received: .....  
Ref. .... Reported to the Unit: Yes/No ....  
Date Reported: ..... Ref .....



## APPENDIX 2 - ML&TF RISK ASSESSMENT REPORT

### INFORMER'S DETAILS

Name: ..... Tel: .....  
Department: ..... Fax: .....  
Position: .....

### CLIENT'S DETAILS

Name: .....  
Address: .....  
.....  
Date of Birth: ..... Tel: .....  
Occupation: ..... Fax: .....  
Details of Employer: .....  
Passport No.: ..... Nationality: .....  
ID Card No.: .....  
Other ID Details: .....

### INFORMATION/SUSPICION

Brief description of activities/transaction: .....  
.....  
.....  
.....  
.....

Reason(s) for suspicion: .....  
.....  
.....  
.....  
.....

Informer's Signature Date .....

### FOR MLCO USE

Date Received: ..... Time Received: .....  
Ref. .... Reported to the Unit: Yes/No ....  
Date Reported: ..... Ref .....



## APPENDIX 3 - SUSPICIOUS TRANSACTION REPORT (STR)

### SUSPICIOUS TRANSACTION REPORT (STR)

Reporting of suspicious transactions or attempted transactions is required under Business Corporations Act, of the Marshall Islands Revised Code entered into force on 1 January 2019.

#### INFORMER'S DETAILS

Name: ..... Tel: .....  
Department: ..... Fax: .....  
Position: .....

#### CLIENT'S DETAILS

Name: .....  
Address: .....  
.....  
Date of Birth: ..... Tel: .....  
Occupation: ..... Fax: .....  
Details of Employer: .....  
Passport No.: ..... Nationality: .....  
ID Card No.: .....  
Other ID Details: .....

#### INFORMATION/SUSPICION

Brief description of activities/transaction: .....  
.....  
.....  
.....  
.....  
.....

Reason(s) for suspicion: .....  
.....  
.....  
.....  
.....

Informer's Signature Date .....

#### FOR MLCO USE

Date Received: ..... Time Received: .....  
Ref. .... Reported to the Unit: Yes/No ....  
Date Reported: ..... Ref .....



## APPENDIX 4 - SUSPICIOUS ACTIVITY REPORT (SAR)

### SUSPICIOUS ACTIVITY REPORT (SAR)

Reporting of suspicious activity is required under Business Corporations Act, of the Marshall Islands  
Revised Code entered into force on 1 January 2019.

#### INFORMER'S DETAILS

Name: ..... Tel: .....  
Department: ..... Fax: .....  
Position: .....

#### CLIENT'S DETAILS

Name: .....  
Address: .....  
.....  
Date of Birth: ..... Tel: .....  
Occupation: ..... Fax: .....  
Details of Employer: .....  
Passport No.: ..... Nationality: .....  
ID Card No.: .....  
Other ID Details: .....

#### INFORMATION/SUSPICION

Brief description of activities/transaction: .....  
.....  
.....  
.....  
.....

Reason(s) for suspicion: .....  
.....  
.....  
.....  
.....

Informer's Signature Date .....

#### FOR MLCO USE

Date Received: ..... Time Received: .....  
Ref. .... Reported to the Unit: Yes/No ....  
Date Reported: ..... Ref .....



## APPENDIX 5 - CASH TRANSACTION REPORT

### CASH TRANSACTION REPORT (CTR)

Reporting of "significant" cash transactions is required by Business Corporations Act, of the Marshall Islands Revised Code entered into force on 1 January 2019.

#### INFORMER'S DETAILS

Name: ..... Tel: .....  
Department: ..... Fax: .....  
Position: .....

#### CLIENT'S DETAILS

Name: .....  
Address: .....  
.....  
Date of Birth: ..... Tel: .....  
Occupation: ..... Fax: .....  
Details of Employer: .....  
Passport No.: ..... Nationality: .....  
ID Card No.: .....  
Other ID Details: .....

#### INFORMATION/SUSPICION

Brief description of activities/transaction: .....  
.....  
.....  
.....  
.....

Reason(s) for suspicion: .....  
.....  
.....  
.....  
.....

Informer's Signature Date .....

#### FOR MLCO USE

Date Received: ..... Time Received: .....  
Ref. .... Reported to the Unit: Yes/No ....  
Date Reported: ..... Ref .....



## APPENDIX 6 - INTERNATIONAL FUNDS TRANSFER REPORT (IFTR)

### INTERNATIONAL FUNDS TRANSFER REPORT (IFTR)

Reporting of electronic funds transfers into or out of Marshall Islands of 100,000\$ or more required by Business Corporations Act, of the Marshall Islands Revised Code entered into force on 1 January 2019.

#### INFORMER'S DETAILS

Name: ..... Tel: .....  
Department: ..... Fax: .....  
Position: .....

#### CLIENT'S DETAILS

Name: .....  
Address: .....  
.....  
Date of Birth: ..... Tel: .....  
Occupation: ..... Fax: .....  
Details of Employer: .....  
Passport No.: ..... Nationality: .....  
ID Card No.: .....  
Other ID Details: .....

#### INFORMATION/SUSPICION

Brief description of activities/transaction: .....  
.....  
.....  
.....  
.....

Reason(s) for suspicion: .....  
.....  
.....  
.....  
.....

Informer's Signature Date .....

#### FOR MLCO USE

Date Received: ..... Time Received: .....  
Ref. .... Reported to the Unit: Yes/No ....  
Date Reported: ..... Ref .....



## APPENDIX 7 - INTERNAL SUSPICIOUS REPORT (ISR)

### INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reporting of Internal suspicious activity are required by Business Corporations Act, of the Marshall Islands Revised Code entered into force on 1 January 2019.

#### INFORMER'S DETAILS

Name: ..... Tel: .....  
Department: ..... Fax: .....  
Position: .....

#### CLIENT'S DETAILS

Name: .....  
Address: .....  
.....  
Date of Birth: ..... Tel: .....  
Occupation: ..... Fax: .....  
Details of Employer: .....  
Passport No.: ..... Nationality: .....  
ID Card No.: .....  
Other ID Details: .....

#### INFORMATION/SUSPICION

Brief description of activities/transaction: .....  
.....  
.....  
.....  
.....

Reason(s) for suspicion: .....  
.....  
.....  
.....  
.....

Informer's Signature Date .....

#### FOR MLCO USE

Date Received: ..... Time Received: .....  
Ref. .... Reported to the Unit: Yes/No ....  
Date Reported: ..... Ref .....



## APPENDIX 8 - INTERNAL EVALUATION REPORT (IER)

### INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference: .....

Client's Details: .....

Informer: .....

Department: .....

#### INQUIRIES UNDERTAKEN (Brief Description)

.....  
.....  
.....

#### ATTACHED DOCUMENTS

.....  
.....  
.....  
.....

#### COMPLIANCE DECISION

.....  
.....  
.....

FILE NUMBER .....

COMPLIANCE SIGNATURE .....

DATE .....

## APPENDIX 9 - CLIENT ACCEPTANCE POLICY ('CAP')

### CLIENT ACCEPTANCE POLICY

#### 1. INTRODUCTION

Money Laundering is the participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities including fraud, corruption, organized crime, terrorism, and many other crimes. Predicate offences for money laundering are defined by local law in the diverse jurisdictions. Generally, the money laundering process consists of three stages:

##### **Placement:**

The physical disposal of the money or assets gained from crime. This may include amongst others:

- i) Placing cash on deposit at a bank (often intermingled with a legitimate money to obscure the audit trail), thus converting cash into readily recoverable funds;
- ii) Physically moving cash between countries;
- iii) Making loans in tainted cash to businesses which seem legitimate or are connected with legitimate businesses, thus also converting cash into debt;

##### **Layering:**

Separating the proceeds of criminal activity from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity. This may amongst others include:

- i) Rapid switches of funds between banks and/or countries;
- ii) Use of cash deposits as collateral to support legitimate transactions;
- iii) Switching cash through a network of legitimate business and "shell companies" across several jurisdictions;

##### **Integration:**

Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

Financial institutions may be misused at any point in the money laundering process.

#### 2. CUSTOMER ACCEPTANCE POLICY ON A RISK BASED APPROACH

The Company's customer's acceptance policy on a risk based approach is prepared by the MLCO after detailed assessment of the risks faced by the Company. In this regard the Company applies appropriate measures and procedures, on a risk based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher.

#### 3. CRITERIA OF ACCEPTING NEW CLIENTS

The Company applies customer identification procedures and customer due diligence measures in the following cases:

- When establishing a business relationship;
- When carrying out occasional transactions
- When there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction;
- When there are doubts about the veracity or adequacy of previously customer identification data.

As a minimum requirement, the following criteria have to be met for accepting new clients:

- Identification and verification of the customer (e.g. Proof of identification and residential address)
- Identification and verification of the beneficial owner(s)
- Obtaining information on the purpose and intended nature of the business relationship

Further details on the documents required to open an account can be found on the Company's AML Manual.

#### 4. CRITERIA FOR NOT ACCEPTING CUSTOMERS

Categories of customers who are not acceptable for establishing a business relationship or an execution of an occasional transaction with our Company are the following:

- Clients who fail or refuse to submit, the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification;
- Potential clients that require to open anonymous account;

- Potential new clients that do not appear to be legitimate are declined;
- Shell Banks;
- Politically Exposed Persons (PEPs) – individuals (domestic and foreign) entrusted with prominent public functions, senior executive members of state owned corporations or international organisations and officials of a political party including their immediate family and close associates;
- UBO listed in United Nations Security Council Consolidated List:

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

Further details on not acceptable clients can be found on the Company's AML Manual.

## 5. DORMANT ACCOUNTS POLICY

The Company has adopted the Dormant Account Policy under which an account is classified as Dormant if it remains inactive or non-operational by its holder for a minimum of period of 5 years.

If an account is classified as Dormant then:

- The accounts will be freeze immediately and the Client will not be permitted to undertake any further transaction in such an account.
- The MLCO or other person of compliance function ascertains reasons for non-operation and requests Clients to close the accounts if they are no longer required.

## 6. CUSTOMER CATEGORY

This Section defines the criteria for the categorisation of Clients based on their risk. The MLCO shall be responsible for categorising Clients in one of the following three (3) categories based on the criteria of each category set below:

### i. Low Risk Clients

The following types of Clients can be classified as low risk Clients with respect to the Money Laundering and Terrorist Financing risk which the Company faces provided that the risk for money laundering and terrorist financing is low and there is no suspicion for legitimating income from illegal revenue or terrorism financing:

- (a) credit or financial institution in Marshall Islands or European Union or non-sanctioned third countries;

- (b) listed companies whose securities are admitted to trading on a Regulated Market in a country of the European Economic Area or in a non-sanctioned third country;

- (c) domestic public authorities of Marshall Islands, European Economic Area or in a non-sanctioned third country.

### ii. Normal Risk Clients

Clients can be classified as normal risk Clients with respect to the Money Laundering and Terrorist Financing risk when they do not fall under the 'low risk Clients' or 'high risk Clients'.

### iii. High Risk Clients

The following types of Clients can be classified as high risk Clients with respect to the Money Laundering and Terrorist Financing risk which the Company faces:

- Clients who are not physically present for identification purposes (non-face-to-face Clients);
- Clients whose own shares or those of their parent companies (if any) have been issued in bearer form;
- Politically Exposed Persons (PEPs) – individuals (domestic and foreign) entrusted with prominent public functions, senior executive members of state owned corporations or international organisations and officials of a political party including their immediate family and close associates;
- All non-resident customers – especially customers who are from countries or regions or industries where a high level of crime is known to exist;
- Customers that work in certain industries or occupations where crime is known to exist;
- Industries at higher risk of being associated with money laundering include:
  - those with high earning potential and which are subject to controls and permits – e.g. fishing and logging
  - dealers in precious metals or stones; and
  - legal professionals and accountants who carry out transactions for their clients.
- Non face-to-face customers – e.g. those which operate accounts via electronic means
- Legal persons or arrangements, such as trusts that act as asset holding vehicles.
- any other Clients that their nature entail a higher risk of money laundering or terrorist financing;



- any other Client determined by the Company itself to be classified as such on the basis of its CAP.

Note: Considering the nature of the Company's business, being an online broker, the majority of the Company's clients are Non-Face-to-Face, implying that all of the Company's clients are, by definition, falling under the High Risk Customer category.

## **7. RISK CRITERIA ON MONEY LAUNDERING OR TERRORIST FINANCING**

The MLCO identifies, records and evaluates four main risk criteria when assessing the extent of money laundering and terrorist financing risks. Based on the extent and the combination of the given risk criteria, a risk scoring will be obtained, where it will identify the ranking

of each customer in relation to the risk faced by the Company on money laundering or terrorist financing.

The MLCO considers the following risk criteria:

- Customer risk;
- Country or geographical risk;
- Products and services risk; and
- Other variables such as:
  - the distribution channels and practices of providing services
  - the volume and size of transactions
  - the degree of risk associated with each area of services
  - the country of origin and destination of Clients' funds
  - deviations from the anticipated level of transactions
  - the nature of business transactions.

## APPENDIX 10 - CLIENT IDENTIFICATION, (KYC) DUE DILIGENCE PROCEDURES

### CLIENT IDENTIFICATION, KNOW YOUR CLIENT (KYC) AND DUE DILIGENCE PROCEDURES

#### 1. General

1.1. Kaje Fin Services Ltd is a company incorporated in Marshall Islands under registration no. 83226 having its registered address at Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, Marshall Islands MH96960 (the “Company”)

1.2. This procedure shall govern the relationship between the Company and the Client whereby the Company will provide to the Client and the Client shall receive from the Company investment and ancillary services, in the manner described herein

1.3. The Company applies customer identification procedures, KYC and customer due diligence measures (i.e. prescribed identification process) in the following cases (inter alia):

- When establishing a business relationship;
- When carrying out occasional transactions that exceeds the prescribed threshold specified in the Act whether conducted as a single transaction or by way of two or more transactions that appear to be linked.
- When there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction;
- When there are doubts about the veracity or adequacy of previously customer identification data.
- The prescribed identification process must also be carried out by the Company on:
  - a person conducting a transaction; and
  - a person on whose behalf a transaction is being conducted; and
  - beneficial owner,

if the reporting entity has reasonable grounds to believe that the person is undertaking a transaction on behalf of another person. In addition to the above, the Company must also verify that a person is authorised to undertake the transaction concerned on behalf of the other person. Failure to apply the above, this is an offence punishable upon conviction by:

(a) if the reporting entity is a natural person - a fine not exceeding 100,000\$ or imprisonment not exceeding 15 years, or both; or

(b) if the reporting entity is a body corporate - a fine not exceeding 100,000\$. In the case where the prescribed identification process cannot be carried out then the following must apply:

- (a) the account must not be opened for the person and
- (b) we must not enter into a business relationship with the said person and
- (c) if a business relationship already exists with a person then the existing business relationship must be terminated.

#### 2. Customer Category

This Section defines the criteria for the categorisation of Clients based on their risk. The MLCO shall be responsible for categorising Clients in one of the following three (3) categories based on the criteria of each category set below:

##### i. Low Risk Clients

The following types of Clients can be classified as low risk Clients with respect to the Money Laundering and Terrorist Financing risk which the Company faces provided that the risk for money laundering and terrorist financing is low and there is no suspicion for legitimating income from illegal revenue or terrorism financing:

- (a) credit or financial institution in Marshall Islands or European Union or non-sanctioned third countries;
- (b) listed companies whose securities are admitted to trading on a Regulated Market in a country of the European Economic Area or in a non-sanctioned third country;
- (c) domestic public authorities of Marshall Islands, European Economic Area or in a non-sanctioned third country.

##### ii. Normal Risk Clients

Clients can be classified as normal risk Clients with respect to the Money Laundering and Terrorist Financing

risk when they do not fall under the 'low risk Clients' or 'high risk Clients'.

### **iii. High Risk Clients**

The following types of Clients can be classified as high risk Clients with respect to the Money Laundering and Terrorist Financing risk which the Company faces:

- Clients who are not physically present for identification purposes (non-face-to-face Clients);
- Clients whose own shares or those of their parent companies (if any) have been issued in bearer form;
- Politically Exposed Persons (PEPs) – individuals (domestic and foreign) entrusted with prominent public functions, senior executive members of state owned corporations or international organisations and officials of a political party including their immediate family and close associates;
- All non-resident customers – especially customers who are from countries or regions or industries where a high level of crime is known to exist;
- Customers that work in certain industries or occupations where crime is known to exist;
- Industries at higher risk of being associated with money laundering include:
  - those with high earning potential and which are subject to controls and permits – e.g. fishing and logging
  - dealers in precious metals or stones; and
  - legal professionals and accountants who carry out transactions for their clients.
  - Non face-to-face customers – e.g. those which operate accounts via electronic means
  - Legal persons or arrangements, such as trusts that act as asset holding vehicles.
- any other Clients that their nature entail a higher risk of money laundering or terrorist financing;
- any other Client determined by the Company itself to be classified as such on the basis of its CAP.

Note: Considering the nature of the Company's business, being an online broker, the majority of the Company's clients are Non-Face-to-Face, implying that all of the Company's clients are, by definition, falling under the High Risk Customer category.

### **3. RISK CRITERIA ON MONEY LAUNDERING OR TERRORIST FINANCING**

The MLCO identifies, records and evaluates four main risk criteria when assessing the extent of money laundering and terrorist financing risks. Based on the extent and the combination of the given risk criteria, a risk scoring will be obtained, where it will identify the ranking of each customer in relation to the risk faced by the Company on money laundering or terrorist financing.

The MLCO considers the following risk criteria:

- Customer risk;
- Country or geographical risk;
- Products and services risk; and
- Other variables such as:
  - the distribution channels and practices of providing services
  - the volume and size of transactions
  - the degree of risk associated with each area of services
  - the country of origin and destination of Clients' funds
  - deviations from the anticipated level of transactions
  - the nature of business transactions.

### **4. CRITERIA FOR NOT ACCEPTING CUSTOMERS**

Categories of customers who are not acceptable for establishing a business relationship or an execution of an occasional transaction with our Company are the following:

- Clients who fail or refuse to submit, the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification;
- Potential clients that require to open anonymous account;
- Potential new clients that do not appear to be legitimate are declined;
- Shell Banks;
- Politically Exposed Persons (PEPs) – individuals (domestic and foreign) entrusted with prominent public functions, senior executive members of state owned corporations or international organisations and officials of a political party including their immediate family and close associates;
- UBO listed in United Nations Security Council Consolidated List:

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>



Further details on not acceptable clients can be found on the Company's AML Manual.

## **5. Customer Identification Process:**

The Company in the cases mentioned in section 1 above, must carry out the prescribed identification process.

The identification process to be applied for the following types of customers is as follows:

### **5.1. (a) Physical Person:**

i. collect the following customer information set out in Table A of Schedule 2 of the Regulation as amended from time to time (enclosed herein as Annex 1) ; and

ii. at a minimum collect the following information:

- the customer's full name; and
  - the customer's date of birth; and
  - the customer's residential address; and
  - the customer's occupation; and
  - the purpose and intended nature of the business relationship with the reporting entity and
  - authorization of any person purporting to act for on behalf of the customer and the identity of the person and;
- iii. have an understanding on:
- the purpose and intended nature of the business relationship with the Company and
  - the customer's beneficial ownership and control structure

### **5.2.(b) Legal Person Customer (i.e. Corporate Client): Guidance on Beneficial Ownership Requirements of the Republic of the Marshall Islands Associations Law**

Internationally agreed standards for anti-money laundering and combating the financing of terrorism and for transparency and exchange of information require jurisdictions to ensure the availability of beneficial ownership information for legal entities and arrangements connected to the jurisdiction. The Republic of the Marshall Islands ("RMI") Associations Law ("RMI Associations Law") includes recordkeeping requirements for beneficial ownership information that are in line with these standards and with similar obligations in other leading corporate jurisdictions.

This guidance was prepared by the RMI Registrar of Corporations responsible for non-resident domestic entities ("Registrar"). It is intended to serve as a general overview of how non-resident domestic entities might

comply with the requirement to collect and make available beneficial ownership information under the RMI Associations Law.

This guidance is not intended as a substitute for the RMI Associations Law. It is provided as a courtesy for general information purposes only and should not be construed as legal advice or a substitute for legal counsel. For legal advice or a legal opinion regarding the requirements for beneficial ownership recordkeeping for your non-resident domestic entity, please consult independent counsel.

### **What beneficial ownership records must be kept?**

In addition to reliable and complete accounting records and up-to-date legal ownership records, the RMI Associations Law requires non-resident domestic entities to use all reasonable efforts to obtain and maintain an up-to-date internal record of the entity's beneficial owners.<sup>1</sup> These records may be kept in any form so long as they can be converted into legible written form within a reasonable time, and they must be kept for a minimum of five years. Bearer shares are subject to additional requirements (see What are the requirements for bearer shares? below).

### **Which entities must keep these records?**

All non-resident domestic entities, except publicly-traded companies, are required to keep beneficial ownership records. "Publicly-traded company" is defined in each act of the RMI Associations Law and broadly includes companies listed on securities exchanges as well as their direct and indirect subsidiaries. An entity is a "subsidiary" of another entity if majority-owned by that other entity or included in that other entity's consolidated financial statements.

<sup>1</sup> For reference, see § 80(3) of the Business Corporations Act, § 37(1)(c) of the Revised Partnership Act, § 32(1)(c) of the Limited Partnership Act, and § 22(1)(c) of the Limited Liability Company Act.

### **Who is a "beneficial owner"?**

In all cases, a "beneficial owner" will be a natural person. "Beneficial owner" has the same definition in each act of the RMI Associations Law: the natural person(s) who ultimately owns or controls, or has ultimate effective control of, a legal entity or arrangement, whether directly or indirectly, or on whose behalf such interest in such legal entity or arrangement is held.<sup>2</sup> This definition mirrors the

internationally agreed standards established by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes ("Global Forum") and the Financial Action Task Force ("FATF"). Guidance produced by these organizations on identifying beneficial owners of legal entities may be a helpful resource (see Other Resources below). The FATF Recommendations<sup>3</sup> describe the determination of beneficial ownership information of legal entities as a two-step process:

#### **STEP 1**

(a) Identify the natural persons (if any) who ultimately have a controlling ownership interest in a legal person, and (b) where there is doubt as to whether the persons identified under (a) are the beneficial owners, or where no natural person exerts control through ownership interests, identify the natural persons (if any) exercising control of the legal person through other means.

**STEP 2** Where no natural person is identified under (a) or (b) above, identify the relevant natural person who holds the position of senior managing official.

#### **Step 1(a) – What is a controlling ownership interest?**

A controlling ownership interest will depend on the company's ownership structure. The RMI Associations Law bases a controlling ownership interest on a threshold: holding more than 25% of the interests or voting rights in a legal entity. Thus, the starting point in most cases will be to assess whether one or more persons meet this threshold. The threshold may be achieved through direct or indirect ownership.

#### **What is direct ownership?**

An interest or voting right held and controlled by a natural person in his/her own name is directly owned by that natural person. Direct ownership is generally recorded in a share register, register of members or partners, or other register of ownership interests. An interest or right held jointly by natural persons may also be considered directly owned.

2 For reference, see § 80(3)(f) of the Business Corporations Act, § 37(1)(c)(v) of the Revised Partnership Act, § 32(1)(c)(v) of the Limited Partnership Act, and § 22(1)(c)(v) of the Limited Liability Company Act. 3 FATF (2012-2018), International Standards on Combating Money Laundering and the Financing of Terrorism &

Proliferation, available at: [www.fatf-gafi.org/recommendations.html](http://www.fatf-gafi.org/recommendations.html).

#### **What is indirect ownership?**

Indirect ownership may occur through a chain of companies or through a nominee shareholder arrangement. Where a share or right is held indirectly, the chain of ownership or nominee arrangement must be looked through to identify the underlying natural persons with a controlling ownership interest. Only natural persons can be "beneficial owners" under the RMI Associations Law. Where the holder of an interest or voting right is a legal entity, the direct owners of that shareholder-entity must be considered. Where one or more of these are also legal entities, the direct owners of these shareholder-entities must be considered too. This process should be continued until a determination can be made as to whether any natural person in the ownership chain meets the 25% threshold for the company in question.

#### **EXAMPLE**

The shares of Corporation A are 10% held by Corporation B and 90% held by Corporation C. Corporation B is 100% owned and controlled by Individual 1. Corporation C is owned and controlled 25% by Individual 1 and 75% by Individual 2. In this case, Individual 1 and Individual 2 are each an indirect owner of Corporation A. Corporation A is ultimately owned and controlled 32.5% by Individual 1 and 67.5% by Individual B. Both Individual 1 and Individual 2 exceed the 25% ownership threshold, so both are "beneficial owners" of Corporation A.

Similarly, shares held by a nominee on behalf of another person must be treated as belonging to that other person, not the nominee.

#### **EXAMPLE**

The shares of Corporation D are 100% held by Individual 3. Individual 3 holds the shares as a nominee on behalf of Individual 4 under the terms of a nominee arrangement. The shares must be treated as belonging to Individual 4, not the nominee. Individual 4 therefore exceeds the 25% ownership threshold and is the "beneficial owner" of Corporation D.

#### **What if no natural person meets the 25% threshold?**

Even if there is no natural person meeting the controlling ownership interest threshold, there may be control through other ownership means. Shareholders may collaborate to

increase a person's level of control through formal or informal agreements. If no natural person meets the 25% threshold, or if there is doubt as to whether a natural person meeting the threshold is the true "beneficial owner," any shareholder agreements, powers to appoint senior management, convertible stock, or outstanding debt that is convertible into voting equity should be considered. A natural person exercising indirect control over the legal entity through one or more of these other ownership means may be considered a "beneficial owner." **EXAMPLE**

The shares of Corporation E are held by 10 shareholders, each with 10% of the ownership and voting rights. All hold Class B shares except Individual 5, who holds Class A shares. Corporation E's articles of incorporation give Class A shares veto power over any sale of Corporation E's sole asset and any change to the nature of Corporation E's business. Individual 5, as the sole holder of Class A shares, may be considered the "beneficial owner" of Corporation E.

#### **Step 1(b) – What is control through other means?**

The RMI Associations Law states that if no natural person exerts control through ownership interests, the natural persons who exercise control through management or other means will be regarded as the "beneficial owner." Other means may include control through personal connections, the financing of the company, family relationships, historical or contractual associations, or default by the company on certain payments. There may be a presumption of control, even if not exercised, where a natural person uses, enjoys, or benefits from the assets of the legal person.

If no natural person exerts control through ownership interests, or if there is doubt as to whether the natural persons exerting control through ownership interests are the true "beneficial owners," a natural person exercising control of the legal entity through one of these other means may be considered a "beneficial owner."

#### **EXAMPLE**

Corporation F was founded, owned, and operated by Individual 6. Individual 6 has retired and transferred the shares of Corporation F in equal 16.667% proportions to her six children, none of whom exert control through ownership means. Though no longer officially involved, Individual 6 still regularly exerts substantial influence over

the decisions of board and the votes of her children as shareholders. Individual 6 may be considered the "beneficial owner" of Corporation F.

#### **Step 2 – Who is a senior managing official?**

As noted above, the RMI Associations Law states that if no natural person exerts control through ownership interests, the natural persons who exercise control through management or other means will be regarded as the "beneficial owner." Natural persons who may exercise control through positions held within a legal entity include those responsible for strategic decisions fundamentally affecting the entity's business practices or strategic direction and those with executive control over the entity's daily affairs. These may include directors (but not nominee directors), managers, or executive officers.

If no natural person exerts control through ownership interests or other means discussed above, the natural person(s) exercising control through management positions held within a legal entity may be considered "beneficial owners."

#### **Who is not a "beneficial owner"?**

A legal entity or arrangement is not a "beneficial owner" under the RMI Associations Law. Only a natural person may be a "beneficial owner." A nominee is not a "beneficial owner" under the RMI Associations Law. Shares held by a

nominee on behalf of another person must be treated as belonging to that other person, not the nominee. Similarly, persons acting on behalf of another person as a nominee director is not a "beneficial owner."

#### **What are the requirements for bearer shares?**

Existing and newly formed non-resident domestic corporations are permitted to issue bearer shares under the § 42(2) of the Business Corporations Act.

Bearer shares are subject to additional recordkeeping requirements, but these requirements are straightforward: the holders and beneficial owners of bearer shares must be recorded with the registered agent for non-resident domestic entities (the "Registered Agent") in the RMI. The validity, rights, and privileges of bearer shares and any transfer of bearer shares are conditional on this recordation. §§ 42(2) and 80(3)(c) of the Business Corporations Act. "Beneficial owner" has the same meaning as specified above (see Who is a "beneficial

owner"? and Who is not a "beneficial owner"?), but here the Business Corporations Act refers to the "beneficial owners of [the] bearer shares" rather than the "beneficial owners of the corporation."

#### **EXAMPLE**

The articles of incorporation of Corporation G authorize 100 registered and/or bearer shares. The directors authorize the issuance of 99 registered shares and 1 bearer share. Individual 7 purchases the 99 registered shares for his own benefit. Corporation H purchases and holds the 1 bearer share. Corporation H is 100% owned and controlled by Individual 8.

To be valid, and for Corporation H to exercise any rights or privileges as a holder of the bearer share, the required records must first be recorded with the Registered Agent. Corporation H should be recorded as the holder of the share and, unless Corporation H holds the share under a nominee or similar arrangement, Individual 8 should be recorded as the beneficial owner of the share.

Bearer share information may initially be recorded with the Registered Agent by completing the Declaration of Holders and Beneficial Owners of Bearer Shares. For any transfer after the initial recordation, the Declaration of Transfer of Bearer Shares may be used to record the necessary information on the new holders and beneficial owners of the shares with the Registered Agent. The Registered Agent adheres to strict data privacy requirements.

#### **How should entities obtain ownership information?**

The RMI Associations Law obligates the legal and beneficial owners of non-resident domestic entities to provide the required ownership details. Non-resident domestic entities are required to use all reasonable efforts to notify their legal and beneficial owners of their obligation to provide the information required to be kept by the entity. This requirement may be fulfilled through an annual written request for the requisite ownership details. Entities are entitled to rely on beneficial ownership details provided in response to these written requests unless the entity has reason to believe the responses are misleading or false.

#### **How is compliance monitored?**

Under internationally agreed standards, compliance with beneficial ownership recordkeeping requirements must be

monitored. To ensure the RMI meets its international obligations, the Registered Agent has been authorized under the RMI Associations Law to audit compliance with recordkeeping requirements. The Registered Agent may request beneficial ownership records in connection with its audit functions, and upon such a request, records must be provided to the Registered Agent in the RMI within 60 days. In addition, the RMI Associations Law requires non-resident domestic entities, except publiclytraded companies, to make an annual attestation that records are being maintained as required. For ease of use, the attestation has been integrated into the Registrar's formation and annual invoicing processes.

#### **What are the penalties for non-compliance?**

Knowingly or recklessly failing to maintain records as required under the RMI Associations Law is punishable by a substantial fine, forcible annulment, or both. There is an exception to liability for failure to maintain beneficial ownership information where all reasonable efforts have been undertaken to obtain and maintain the required information. Failure to produce records to the Registered Agent within 60 days upon request, failure to make attestations as required, willfully maintaining or producing false or misleading records, and making false or misleading attestations are also punishable by a substantial fine, forcible annulment, or both.<sup>6</sup> With respect to bearer shares, the validity, rights, and privileges of bearer shares are conditional on recordation of the required ownership information with the Registered Agent. Bearer shares that do not comply become invalid and must be cancelled by the corporation.<sup>7</sup> Other Resources The Trust Company of the Marshall Islands, Inc., Republic of the Marshall Islands Associations Law, available at: <http://www.registeriri.com/index.cfm?action=page&page=31>. FATF (2012-2018), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, available at: [www.fatfgafi.org/recommendations.html](http://www.fatfgafi.org/recommendations.html) FATF (2014), FATF Guidance: Transparency and Beneficial Ownership, available at: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/transparencyand-beneficial-ownership.html>. OECD, Exchange of Information on Request: Handbook for Peer Reviews 2010-2016, 3d Edition, available at:

<http://www.oecd.org/tax/transparency/global-forum-handbook2016.pdf>.

### **5.3. (c) Legal Arrangement Customer:**

i. collect the following customer information set out in Table A of Schedule 2 of the

Regulation as amended from time to time (enclosed herein as Annex 1) ; and

ii. at a minimum collect the following information:

- the full business name of the customer; and
- the full business address of the customer; and
- the type of customer; and
- the country in which the customer was established; and
- the full name and address of each of the trustee or similar positions of the customer; and
- the full name and address of each of the settlor or similar position, the protector (if any) or similar position and each beneficiaries (including through a chain of control/ownership) of the customer; and
- the authorization of any person purporting to act for or on behalf of the customer, and the identity of the persons; and
- the purpose and intended nature of the business relationship with the reporting entity and;

iii. have an understanding on:

- the purpose and intended nature of the business relationship with the Company and
- the customer's beneficial ownership and control structure

### **3. Customer Verification Process**

#### **3.1. General**

The Company must carry out the prescribed verification process. The evidence of verification required should be obtained from documents issued by reputable, reliable and independent sources. Customer verification must be conducted within the prescribed event, circumstance and/or period timeframes as follows:

- i. Prescribed event; if there is suspicion that the customer is involved in or that the transaction involves ML, TF or other serious offences, the Company must verify the identity of the customer undertaking the transaction within 2 working days;
- ii. Prescribed circumstance: if there is suspicion on reasonable grounds that the customer is not the person he

or she claims to be, the Company must, within 3 working days; (i) collect the necessary identification information of the customer; or (ii) verify the customer's identification.

iii. Prescribed period: the Company must verify the identification of the customer within 5 working days except (i) if the Company's ML&TF risk is low or medium low, it must verify within 15 working days or (ii) if it reasonably believe that by doing so may inform the customer of the suspicions, the Company is exempted from conducting the verification process and must file a STR/SAR to the Republic of the Marshall Islands The Office Of The Registrar of Corporations.

### **6.1..Verification Process:**

The verification process to be applied for the following types of customers is as follows:

#### **(a) Physical Person:**

The following combinations of documents from the list below are acceptable as verification for a physical person as per the Law and Regulations:

- i. Two 'Category A' documents, (enclosed herein as Annex 2) or
- ii. One 'Category A' document and two 'Category B' (enclosed herein as Annex2) letters, or
- iii. Three 'Category B' letters.

The Company ensures that customers provide at least one document capable of serving as photo identification. This may include a photo that is signed and verified by a person listed in 'Category B'. The Company may waive this photo requirement for customers where it is satisfied the person's identity can be adequately verified through other means. The Company adopts a risk-based approach. 'Category A' documents are more robust than 'Category B' documents. When verifying an individual's identity, a 'top-down' approach should be used by asking individuals to provide 'Category A' documents first, before drawing on 'Category B' documents. The process of identification should be documented and the Company should state in writing why the decision was made to accept Category B documents to verify an individual's identity.

#### **\*General Practice:**

Without prejudice of the above, the Company as a general practice will aim to collect the following documents in relation to:

- Name verification:

- Valid Passport
- National ID Card
- Current photo-card driving licence

The indicated documents should be valid and not less than 6 months from expiry date

- Address Verification:

- Proof of recent utility bill (water, electricity, gas etc.)
- Bank Statement
- Credit Card Monthly Statement
- Customer's tax identification number, Social Security Number or Government Service and Insurance System Number

The indicated documents should be valid and not more than 3 months old. Further to the above, the Company performs at all times a background check on the respective individual through various sources and databases so as to ensure that the client is neither a PEP, or involved in a ML or TF or other predicate offence. Such evidence is kept in the Company's records created for the respective individual.

#### **6.2.(b) Legal Person Customer (i.e. Corporate Client):**

The following documents should be obtained as verification for legal person customer:

- i. Certificate of incorporation and any change of name certificates; where the corporate body is incorporated outside Marshall Islands, such certificates should be certified or, where the certificates form part of a business transaction record, such certificates should be notarized.
- ii. Certificate of Directors
- iii. Certificate of Shareholders up to the UBO(s)
- iv. Certificate of By-Laws (Memorandum and Articles of Association)
  - i. Address of the registered office and name and address of registered agent, if applicable
  - ii. Address of principal place of business
  - iii. The originals or certified copies of any or all of the foregoing documents where required, should be produced and submitted for verification:
    - Sworn Statement as to existence or non-existence of beneficial owners
    - Appropriate Board of Directors' resolutions and signed application forms or account opening, identifying the

authorized signatories or principal officers of the corporation authorised to trade and their authorities and specimen signatures

iv. Board Resolution authorizing the corporation to open the account with the Company

v. Latest Audited Financial Statements (if applicable)

Verification of UBO(s), directors, authorized representatives: It is important to note that the verified identity of each of the beneficial owners of the company who hold an interest of 10% or more in the company and/or the persons on whose instructions the directors, the signatories on the account or the individuals authorized to deal with the reporting entity are empowered to act must be obtained at all times.

Further to the above, the Company should ensure that the potential corporate client has not been or is not in the process of being dissolved, struck off, wound-up or terminated. This can be done through the collection of Certificate of Good Standing or Non-Bankruptcy letter or through a search with the use of different databases and sources so as for the Company to reasonably establish that the potential corporate client is not in the process of any of the abovementioned.

(c) Partnerships:

Similar documents as described in section (b) above (i.e. corporate clients) must be collected and also, the identity of each individual partner who is an account signatory or who is authorised to give instructions to the reporting entity, should be verified as if he or she is a prospective direct personal client. In the case of a limited partnership, the identity of a limited partner need not be verified unless he or she is a significant investor (i.e. has contributed more than 10% of the total capital of the partnership).

(d) Legal Arrangements:

The identification of trustees or similar positions, settlors or similar positions, protectors or similar positions, any person having power to appoint or remove trustees or similar positions and any person (other than the settlor or similar positions) who has provided funds to the settlement should be verified as direct prospective clients (individual or corporate, as appropriate). In addition, the following should be obtained and understood:

- i. Evidence verifying proper appointment of trustees or similar positions, e.g. copy extracts from the Deed of Trust or a letter from a lawyer verifying the appointment;
- ii. Details of the nature and purpose of the arrangement; and
- iii. Details of the source of funds.

Furthermore, the Company should also obtain and verify the identity of the beneficiaries or the principal beneficiaries of a legal arrangement. If the legal arrangement is complex, it is accepted that this will not always be possible or necessary depending on the reporting entity's judgement of the money laundering risk involved. However if such a situation arises, the Company takes appropriate steps to satisfactorily identify the beneficiaries of the legal arrangement.

## **7. Certification of Documents**

### **(a) Suitable Certifiers:**

A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated bank, trust company or trustee company, notary public or member of the judiciary. The certifier should sign the copy document (printing his or her name clearly underneath) and clearly indicate his position or capacity on it together with a contact address and telephone number.

The list of suitable certifiers is not intended to be exhaustive and Company exercises due caution when considering certified copy documents, especially where such documents originate from a country perceived to represent a high risk of financial crime or money laundering or from unregulated entities in any jurisdiction. Where certified copy documents are accepted, it is the Company's responsibility to satisfy itself that the certifier is appropriate. In all cases, the Company should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate or other document.

### **(b) Reliance on Other Institutions to Verify Identity:**

In those instances where the Company relies on due diligence conducted by another Institution it ensures that the KYC procedures of that other Institution are not weaker to those established by the Company or those applicable under the Law and Regulations.

## **8. Changes to Customer Status and Operations**

The Company takes all necessary actions using the identification procedures and measures to provide due diligence, in order to collect the appropriate evidence in cases of:

(a) Changed to the customer identification standards such as:

- i. Change of directors/secretary
- ii. Change of registered shareholders and or actual beneficiaries
- iii. Change of registered office
- iv. Change of trustees
- v. Change of corporate name and/or tradename
- vi. Change of main trading partners and/or significant new business

(b) A material change in the way an account is operated such as:

- i. Change of persons authorized to handle its account
- ii. Request for opening a new account in order to provide new investment services and/or financial instruments.

(c) A significant transaction that appears to be unusual and/or significant than the usual type of trade and profile of the client

## **5. Enhanced Client Identification and Due Diligence (High Risk Clients)**

### **5.1. General Provisions:**

The Company shall apply enhanced due diligence measures, in addition to the measures referred to with respect to the Clients categorised as high risk Clients.

The following are examples of high risk customers:

- Politically Exposed Persons (PEPs) – individuals (domestic and foreign) entrusted with prominent public functions, senior executive members of state owned corporations or international organisations and officials of a political party including their immediate family and close associates.
- All non-resident customers – especially customers who are from countries or regions or industries where a high level of crime is known to exist.
- Customers that work in certain industries or occupations where crime is known to exist.
- Non-face to face clients
- Legal persons or arrangements, such as trusts that act as asset holding vehicles.

In general, in case of High Risk Clients the Company takes reasonable measures to:

- Collect and verify additional information on the intended nature of the business relationship;
- Collect and verify information on the source of funds or source of wealth of the customer;
- Collect and verify information on the ultimate beneficial owner of the customer;
- Collect and verify information on the reason for intended or performed transactions;
- Obtaining the senior management's approval of the reporting entity to commence or continue the business relationship;; and
- conduct regular and ongoing monitoring of the customer's transactions.

#### **9. Non face-to-face Clients:**

Considering the nature of the Company's business, being an online broker, all of the Company's clients are Non-Face-to-Face, implying that all of the Company's clients are, by definition, falling under the High Risk Customer category.

The Company shall apply the following with respect to non face-to-face Clients:

- i. Telephone contact with the Client at his home or office on a telephone number which has been verified from independent and reliable sources. During the telephone contact, the Company shall confirm additional aspects of the identity information submitted by the Client during the procedure of opening his account.
- ii. Collection of identification and documentation in original form or true copy of the original, where the certification is made by the Company in cases where it establishes the customer's identity itself, once the original is presented thereto, or
- iii. Requisition of additional documents to complement those which are required for face-to-face customers;
- iv. Seeking verification of the source of funds for the initial deposit, including sighting documentary evidence confirming the source of funds (e.g. submission of Income Tax Return and/or bank statement or any proof of income)

#### **10. Politically Exposed Persons (PEPs)**

Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose the Company to significant reputational and/or legal risks.

Politically Exposed Persons ("PEPs") are domestic and foreign individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and international organisations, and important political party officials. As part of the Company's duty to verify a customer's identification, the Company:

- i. gathers sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP or is an immediate family member or close associate of a PEP.
  - ii. investigates the source of funds before accepting a PEP or a close associate or immediate family member of a PEP.
- The decision to establish a business relationship with a PEP should be taken at a senior management level.

#### **11. Sanction Listed Client**

Marshall Islands implement United Nations Security Council Consolidated List.

Business relationships with individuals listed in UN Sanctions list and with persons or companies clearly related to them may expose the Company to significant reputational and/or legal risks. Regarding this risk Customers who are Listed in UN Sanctions list are not acceptable for establishing a business relationship or an execution of an occasional transaction with our Company. On the account opening procedure, customer name, company name will be scanned in the United Nations Security Council Consolidated List (<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>)

The Consolidated List includes all individuals and entities subject to measures imposed by the Security Council. The inclusion of all names on one Consolidated List is to facilitate the implementation of the measures, and neither implies that all names are listed under one regime, nor that the criteria for listing specific names are the same. For each instance where the Security Council has decided to

impose measures in response to a threat, a Security Council Committee manages the sanctions regime. Each sanctions committee established by the United Nations Security Council therefore publishes the names of individuals and entities listed in relation to that committee as well as information concerning the specific measures that apply to each listed name.

During the CDD and the KYC procedure, company uses for Sanction check

- United Nations Security Council Consolidated List  
(<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>)
- Uses the FATF's List Jurisdictions under Increased Monitoring - 21 October 2022
- OFAC sanction list  
(<https://sanctionssearch.ofac.treas.gov/>)
- Consolidated list of persons, groups and entities subject to EU financial sanctions  
(<https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en>)

## 12. Ongoing monitoring

Company runs a customer database once in 6 months for the updates in the 5. mentioned sanction lists.

## 13. Introduced Business

In the case where the Company relies on an intermediary third party in relation to due diligence procedures, the Company must:

- i. Satisfy itself that the intermediary is regulated and supervised and has measures in place to comply with the requirements of Part 2 of the AML&CTF Act;
- ii. Ensure that copies of identification documents and other relevant documents will be made available to it upon request without delay;
- iii. Immediately obtain the information required for customer due diligence requirements as described in the Manual

The Company uses the following criteria to determine whether it can rely upon an introducer:

- i. It must comply with the minimum customer due diligence practices identified in the AML&CTF Act, the AML&CTF Regulation and this Guideline;
- ii. The customer due diligence procedures of the introducer should be as rigorous as those which the Company would have conducted itself for the customer;
- iii. The Company must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer by auditing and reviewing the systems put in place by the introducer;
- iv. The Company must have a written agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- v. As required by the AML&CTF Act, all relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the Company, which must carefully review the documentation provided to ensure that it has met its statutory obligations under the AML&CTF Act. (Such information must be available for review by supervisory authorities such as the RSI Bank Commission of Marshall Islands, where appropriate legal authority has been obtained).
- vi. The Company should conduct periodic reviews to ensure that an introducer that it relies on continues to conform to the criteria set out above.

## 14. Account operated by a third party

Once an account is opened for a client, particular care shall be taken in cases where instructions for transactions on behalf of said client is being made by another person or party. The Company requires for such person or party must be formally authorized by the client (owner of account) to make such transactions on his/her behalf and as such the Company requires the necessary documentation such as

- Special Power of Attorney (SPA) or;
- Duly signature-verified authorization given by clients (e.g. authorized to place an order, up to what amount and authorization to request and receive withdrawal).

## 15. Nominees or agents of third persons

The Company shall take reasonable measures to obtain adequate documents, data or information for the purpose

of establishing and verifying the identity, according to the procedures set in the Manual:

- (a) the nominee or the agent of the third person, and
- (b) any third person on whose behalf the nominee or the agent is acting.

In addition, the Company shall obtain a copy of the authorisation agreement that has been concluded between the interested parties.

## **16. ON-GOING MONITORING PROCESS**

### **16.1.General:**

The Company aims to have a full understanding of normal and reasonable account activity of its Clients as well as of their economic profile and has the means of identifying transactions which fall outside the regular pattern of an account's activity or to identify complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason. Without such knowledge, the Company shall not be able to discharge its legal obligation to identify and report suspicious transactions to the appropriate bodies.

The constant monitoring of the Clients' accounts and transactions is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing. The monitoring system relies both on automated monitoring and where appropriate, manual monitoring by the staff of the compliance function.

### **16.2.Procedures:**

The procedures and intensity of monitoring accounts and examining transactions are based on the level of risk and, as a minimum, achieve the following:

- (a) Identifying all high risk Clients, as applicable; the Company shall have in place systems or measures and procedures that will enable the Company to produce detailed lists of high risk Clients, so as to facilitate enhanced monitoring of accounts and transactions, as deemed necessary;
- (b) Detecting unusual or suspicious transactions that are inconsistent with the economic profile of the Client for the purposes of further investigation.
- (c) The investigation of unusual or suspicious transactions from the employees who have been appointed for that purpose; the results of the investigations are recorded in a

separate memo and kept in the file of the customer concerned;

- (d) all necessary measures and actions must be taken, based on the investigation findings of point (c), including any internal reporting of suspicious transactions/activities to the MLCO;

(e) Ascertaining the source and origin of funds credited to accounts.

(f) Identifying transactions which, as of their nature, may be associated with money laundering or terrorist financing Transactions executed for the customer are compared and evaluated by the MLCO and staff of the compliance function against:

- The anticipated account's turnover;
- The usual turnover of the activities/operations of the customer;
- The data and information kept for the customer's economic profile.

The Company introduces and implements the use of appropriate and proportionate IT systems, which include:

- adequate automated electronic management information systems which will be capable of supplying the Board of Directors and the MLCO, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of Client accounts and transactions based on the assessed risk for money laundering or terrorist financing purposes, in view of the nature, scale and complexity of the Company's business and the nature and range of the investment services undertaken in the course of that business;
- automated electronic management information systems that may be used to extract data and information that is missing regarding the Client identification and the construction of a Client's economic profile;
- for all accounts, automated electronic management information systems to add up the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This can be done by setting limits for a particular type, or category of accounts (e.g. high risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account

the economic profile of the Client, the country of his origin, the source of the funds, the type of transaction or other risk factors. The Company shall pay particular attention to transactions exceeding the above mentioned limits, which may indicate that a Client might be involved in unusual or suspicious activities.

### **16.3.Red Flags – Examples:**

Examples of Red Flags are:

- Transactions with no discernible purpose or are unnecessarily complex.
- Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the Client.
- The transactions or the size of the transactions requested by the Client do not comply with his usual practice and business activity.
- Large volume of transactions and/or money deposited or credited into an account when the nature of the Client's business activities would not appear to justify such activity.
- The Business Relationship involves only one transaction or it has a short duration.
- There is no visible justification for a Client using the services of a particular financial organisation. For example the Client is situated far away from the particular financial organisation and in a place where he could be provided services by another financial organisation.
- There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).
- There are frequent small purchases of a particular financial instrument by a Client who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the Client's instructions, in an account other than his usual account.
- Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.
- Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.

- The settlement of any transaction but mainly large transactions, in cash.
- Settlement of the transaction by a third person which is different than the Client which gave the order.
- Instructions of payment to a third person that does not seem to be related with the instructor.
- Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.
- A Client is reluctant to provide complete information when establishes a Business Relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with financial organisations, names of its officers and directors, or information on its business location. The Client usually provides minimum or misleading information that is difficult or expensive for the financial organisation to verify.
- A Client provides unusual or suspicious identification documents that cannot be readily verified.
- A Client's home/business telephone is disconnected.
- A Client that makes frequent or large transactions and has no record of past or present employment experience.
- Difficulties or delays on the submission of the financial statements or other identification documents, of a Client/legal person.
- A Client who has been introduced by a foreign financial organisation, or by a third person whose countries or geographical areas of origin do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.
- Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).
- The stated occupation of the Client is not commensurate with the level or size of the executed transactions.
- Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

- Unexplained inconsistencies arising during the process of identifying and verifying the Client (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).
- Complex trust or nominee network.

## **17. DEPOSIT AND WITHDRAWAL REQUIREMENTS**

### **17.1. Deposits:**

The Company monitors funding from various funding sources to the accounts of account holders. The Company will NOT accept funds via a third party.

(a) Wire transfer:

In the case of deposit through the means of wire transfer the Company must proceed with Owner Verification procedure which means that it must be satisfied that the Depositor's Details (i.e. name) match those of the account holder. This is achieved with the provision of Deposit Confirmation/Slip (Swift) by the respective client.

(b) Credit/Debit Card:

In the case of deposit via debit/credit card, prior to crediting funds into client's account:

- Client must provide a copy of the front and the back side of the credit card used;
- Client to cover all sensitive information from the front and the back side of the credit card apart from:
  - The cardholder's name,
  - bank of issue and expiry dates,
  - and the first and last 4 digit of the CVV number should be covered at all times.

### **17.2. Withdrawals**

The withdrawal process detailed below is structured so as to make sure that funds are securely sent back to their originating source and beneficiary. The Company does not allow withdrawals to third parties.

Withdrawal Process:

i. The client must complete a withdrawal request containing their correct account information. The said request can be submitted either online through client's portal or manually.

ii. All withdrawal forms whether online or otherwise are submitted to the Company's accounts department for processing. The Accounts Department confirms the account balance, verifies there are no any withdrawal restrictions on the account and then approves the withdrawal request, pending compliance approval.

iii. The Accounts department ensures and verifies that original funds are withdrawn via the same method of deposit and to the originate source.

iv. The Accounts department further checks and examines the withdrawal request against the customer's deposit history so as to ensure there is no suspicious activity and verifies bank account on file

v. Withdrawal requests are approved by compliance are processed by the Accounts Department and funds are released to the client

vi. In case of a red flag or whether a specific withdrawal has been flagged as suspicious, the withdrawal is placed on hold, pending further investigation by the Company's Compliance Officer and compliance staff.

vii. The Company and the Accounts department will work closely with the Compliance Officer and compliance function in general to determine whether further actions are needed and if any relevant regulatory bodies need to be informed.

### **17.3. Cash Deposits or Withdrawals**

The Company neither accepts cash deposits nor disburses cash under any circumstances.

## **Schedule 2 Table A - Collection of Customer Information**

### **18. INDIVIDUAL IDENTIFICATION**

18.1.1.. In relation to a customer who is an individual:

- (a) the customer's name;
- (b) the customer's residential address;
- (c) the customer's date of birth;
- (d) any other name that the customer is known by;
- (e) the customer's country(ies) of citizenship;
- (f) the customer's country(ies) of residence;
- (g) the customer's occupation or business activities;
- (h) the nature of the customer's proposed relationship with the reporting entity - including: • the purpose of specific

transactions; or • the expected nature and level of transaction behavior.

- (i) the income or assets available to the customer;
- (j) the customer's source of funds including the origin of funds;
- (k) the customer's financial position;
- (l) the beneficial ownership of the funds used by the customer;
- (m) the beneficiaries of the transactions being facilitated by the reporting entity on behalf of the customer including the destination of funds.

18.1.2. In relation to a customer who is a sole trader:

- (a) The full name of the sole trader as registered under Republic of the Marshall Islands The Office Of The Registrar of Corporations
- (b) The full address of the business or customer's residential address;
- (c) Business License, CT number issued to the business;
- (d) Nature of the business activities conducted by the sole trader;
- (e) Beneficial owners of the business.

## 18.2.LEGAL PERSON

18.2.1. In relation to a customer who is a company:

- (a) the full name of the company as registered by Office Of The Registrar of Corporations;
- (b) the full address of the company's registered office;
- (c) the full address of the company's principal place of business (if any);
- (d) the Republic of the Marshall Islands The Office Of The Registrar of Corporations , Business License and CT number issued to the company;
- (e) company structure;
- (f) the name of each director of the company;
- (g) the name of the company secretary
- (h) the date upon which the company was registered by Republic of the Marshall Islands The Office Of The Registrar of Corporations;
- (i) the name of any company secretary;
- (j) the nature of the business activities conducted by the company;
- (k) the full name and address of each beneficial owner of the company

18.2.2. In relation to a customer who is a foreign registered Company:

- (a) full name of the foreign company;
  - (b) the full address of the company's registered office and registered agent in Marshall Islands;
  - (c) the full address of the company's principal place of business in Marshall Islands;
  - (d) the company structure;
  - (e) name of each company director and secretary;
  - (f) nature of the business activities conducted by the company:
  - (f)a) in country of registration, formation, incorporation;
  - (f)b) in Marshall Islands;
  - (g) name and address of beneficial owners of the company;
  - (h) the country in which the company was formed, incorporated or registered;
  - (i) whether the company is registered by the relevant foreign registration body and if so, its the company structure;
  - (j) the name of the relevant foreign registration body
  - (k) any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;
  - (l) the date upon which the company was formed, incorporated or registered in its country of formation, incorporation or registration;
  - (m) the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body.
- 18.2.3. In relation to a customer who is an unregistered foreign Company:
- (a) the full name of the company;
  - (b) full address of the company's registered office and registered agent in Marshall Islands;
  - (c) the full address of the company's principal place of business in Marshall Islands;
  - (d) company structure;
  - (e) name of each company director and secretary;
  - (f) the country in which the company was formed, incorporated or registered;
  - (g) whether the company is registered by the relevant foreign registration body and if so:
    - i. any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation m registration;

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

iii. company structure;

(h) the name of the relevant foreign registration body;

(i) the date upon which the company was formed, incorporated or registered in its country of formation, incorporation or registration

(j) the full address of the company's principal place of business in that country; and

(k) the name and address of any beneficial owner of the company.

18.2.4. In relation to a customer who is a partner of a partnership:

(a) the full name of the partnership;

(b) the full business name of the partnership as registered under

(c) Republic of the Marshall Islands The Office Of The Registrar of Corporations ;

(d) the Business' license and VAT number

(e) the country in which the partnership was established;

(f) the full name and residential address of any partner;

(g) the respective share of each partner in the partnership;

(h) the nature of business of the partnership;

(i) the date upon which the partnership was established.

18.2.5. In relation to a customer who is an incorporated association:

(a) the full name of the association as registered under Republic of the Marshall Islands The Office Of The Registrar of Corporations ;

(b) the full address of principal place of administration or registered office (if any) or the residential address of the association's public officer or (if there is no such person) the association's president, secretary or treasurer;

(c) registration number issued by Republic of the Marshall Islands The Office Of The Registrar of Corporations or any unique identifying number issued to the association upon its incorporation;

(d) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association;

(e) country in which the association was incorporated;

(f) the date upon which the association was incorporated;

(g) the objects of the association;

(h) in respect of any member - the information required to be collected from an individual under the reporting entity's customer identification program in respect of individuals; and

(i) the full business name, if any, of the association.

18.2.6. In relation to a customer who is a registered co-operative:

(a) the full name of the co-operative as registered with the Registrar of Cooperatives;

(b) the full address of the co-operatives registered office or principal place of operations (if any) or the residential address of the cooperatives secretary or (if there is no such person) the cooperatives president or treasurer;

(c) any unique identifying number issued to the co-operative upon its registration by the relevant registration body;

(d) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the co-operative;

(e) in respect of any member - the information required to be collected from an individual under the reporting entity's customer identification program in respect of individuals;

(f) the full business name, if any, of the co-operative;

(g) the country or province in which the co-operative is registered;

(h) the date upon which the co-operative was registered;

(i) the objects of the co-operative; and in a certified copy or certified extract of the rules of the co-operative.

18.2.7. In relation to a customer who is a government body:

(a) the full name of the government body;

(b) the full address of the government body's principal place of operations;

(c) whether the government body is an entity or emanation, or established under legislation;

(d) information about the ownership or control of a government body that is an entity or emanation or established under legislation of a foreign country; and

(e) the name of any legislation under which the government body was

Established

## 19. CATEGORIES OF OFFICIAL DOCUMENTS

### 19.1. CATEGORY A - Official Documents acceptable

**19.2. CATEGORY B** - A written reference confirming the customer's full name, date of birth and occupation, from one of the following acceptable referees:

<p><b>CATEGORY A Official Documents</b></p> <ul style="list-style-type: none"> <li>• Current passport (all countries)</li> <li>• Marriage certificate</li> <li>• Educational institution</li> <li>• Current driver's license (all certificates countries)</li> <li>• Student card or registration document for an educational institution (such as a primary or high school)</li> <li>• Government identification documents</li> <li>• Government health card</li> <li>• Certificate of Christening/Baptism</li> <li>• Citizenship certificate</li> <li>• License or permit issued by the Government of the Republic of Marshall Islands</li> <li>• Birth certificate</li> <li>• Employment identification</li> <li>• Employment records</li> <li>• Public utilities record (such as an electricity)</li> <li>• Employment pay slips</li> <li>• Other official records from the Government of the Republic of Marshall Islands</li> <li>• Current records of membership of professional trade organisation</li> <li>• An existing customer who is known favourably to the reporting entity (verified by a reporting entity signature)</li> <li>• Records from a bank (including bank or credit cards such as Visa, Diners, Club, Master Card, an American Express; or statements for an account or credit card)</li> <li>• An existing customer with a bank who has held account with the bank for more than two years</li> <li>• Foreign pensioner's card</li> <li>• Superannuation or provident fund membership card</li> <li>• Marshall Islands work permit</li> <li>• Firearms license</li> <li>• Mortgage or other security document over the customer's property</li> </ul>	<p><b>CATEGORY B</b></p> <p>A written reference confirming the customer's full name, date of birth and occupation, from one of the following acceptable referees:</p> <ul style="list-style-type: none"> <li>• A senior bank employee</li> <li>• An officer in charge of a bank agency</li> <li>• A bank manager</li> <li>• A lawyer or legal practitioner</li> <li>• A registered medical practitioner or dentist</li> <li>• A qualified pharmacist</li> <li>• A Magistrate of a District Court</li> <li>• A landlord of a rented premises where the person lives</li> <li>• A public servant</li> <li>• A Customs or Immigration officer</li> <li>• A Magistrate</li> <li>• A local level Government Councillor</li> <li>• A Notary</li> <li>• A Headmaster of a primary or secondary school</li> <li>• A serving Member of Parliament</li> <li>• A Police officer or commander</li> <li>• An accountant who is a member of an association of accountants</li> <li>• An employee of a reporting entity or cash dealer</li> <li>• A statutory declaration from a</li> </ul>
---	--