ANTI-MONEY LAUNDERING COMPLIANCE MANUAL

XBULLION

Revised November 2020

Table of Contents

SECTION 1. INTRODUCTION & POLICY STATEMENTS

1.1 POLICY

XBULLION, an exempted company incorporated with limited liability in the Cayman Islands, (the "Company") is committed to the enforcement of laws to prevent money laundering, terrorist financing, proliferation and proliferation financing and other illegal transactions. It is the policy of the Company to ensure that high ethical standards are maintained and act in a manner that is in compliance with all laws, regulations, rules and regulatory statements of guidance and principles relevant to its business.

The manual is applicable to all staff of the Company, inclusive of all officers, directors, managers, administrators and support staff and is not limited to individuals working under a contract of employment but also includes temporary and contract staff.

1.2 PURPOSE

The purpose of this Anti-Money Laundering Compliance Manual is to comply with Cayman Islands legislation and regulations, while providing staff with resources to enable them to meet their personal and corporate obligations under the legislative framework in the Cayman Islands for the prevention of money laundering, terrorist financing, proliferation and proliferation financing described in further detail under the section entitled "Legislation Framework" of this manual.

All relevant personnel must be aware of the existence and content of this manual, immediately bringing any anomalies or concerns to the attention of the Anti-Money Laundering Compliance Officer ("AMLCO") and/or Directors as appropriate.

This guidance is not intended to be an alternative to reading the relevant provisions of the Cayman Islands Proceeds of Crime Law (2020 Revision) ("POCL") and the other laws mentioned herein. All staff are to sign a confirmation that they have read and understood the policies and procedures and are aware of their personal obligations. This confirmation will be kept by the AMLCO and updated whenever the manual changes.

The Directors have approved this manual and will be expected to approve any subsequent amendments.

1.2 ANTI-MONEY LAUNDERING POLICY RESPONSIBILITY

Although the Directors retain overall responsibility for all policy and procedures including this manual, the Directors may delegate the resonsiblity for the production and update of this manual to an officer of the Company who is expected to act in consultation with the AMLCO.

The AMLCO will remain informed about current developments in anti-money laundering legislation, regulation and trends and will ensure that appropriate amendments are made to the manual on a timely basis and that all appropriate senior management and the, Directors are duly informed. Senior management of the Company is expected to then inform their staff of the changes. All questions regarding this manual should be addressed initially through the AMLCO or the Anti-Money Laundering Reporting Officer ("MLRO").

Additionally, if any personnel become aware of anomalies in this manual that may be contradictory to current practical procedures, senior management, MLRO, DMLRO and/or AMLCO should be immediately informed. The Company has appointed the following individuals for responsibly of the Anti-Money Laundering program:

Money Laundering Reporting Officer ("MLRO")	Name: Dean Lynee
Deputy Money Laundering Reporting Officer ("DMLRO")	Name: Jennison Nunez
Anti-Money Laundering Compliance Officer ("AMLCO")	Name: Dean Lynee

1.4 PERSONNEL AWARENESS

The Company requires all personnel to be aware of their personal anti-money laundering obligations under the legislation and regulation. All personnel should read and follow the procedures contained in this manual, as failure to maintain adequate awareness and adhere to procedures that are commensurate with an individual's position within the Company may result in internal disciplinary action, diminished compensation and/or termination of employment.

Additionally, in the event that suspicious or unusual activity is detected, subsequent court proceedings may result in suspension and ultimately in criminal prosecution if an individual is found to be negligent in meeting his or her obligations. Regardless of the outcome of court proceedings, if any, the board of directors with the guidance of the AMLCO in conjunction with the MLRO may determine whether an individual has properly met his or her obligations and maintained adequate awareness commensurate with expectations. Failure to meet these obligations may provide grounds for dismissal from the Company.

All principals and personnel, regardless of their level of seniority, will receive regular updates and annual training in current money laundering, terrorist financing and proliferation trends in order to assist them in remaining vigilant so that they are able to detect matters that appear to be unusual in nature, particularly those which might be indicative of illegal activity.

Any concerns relating to an individual's ability to meet personal or corporate obligations, must be brought to the attention of senior management and/or the AMLCO immediately.

SECTION 2. MONEY LAUNDERING & TERRORIST FINANCING

2.1 WHAT IS MONEY LAUNDERING?

Money laundering is the process by which criminals seek to disguise the identity and true source of their illegal income and make it appear legitimate. Criminals launder money so they can avoid detection by law enforcement authorities and make personal use of illicit proceeds – including further criminal activity and investment in legitimate businesses.

2.2 WHAT IS TERRORIST FINANCING?

Terrorist financing can be defined as providing funds to an organization with the intention that they should be used, or the knowledge that they are to be used, to commit a terrorist act. Experts generally believe that terrorist financing comes from two primary sources. The first source is the financial support provided by states or organizations with large enough infrastructures to collect and then make funds available to the terrorist cells. The second major source of funds for terrorist organizations is income derived directly from various "revenue-generating" activities.

While this manual speaks of Money Laundering in general terms, it is important that staff be aware that the financing of terrorism may present itself in a manner similar to that of money laundering or by some other means unique unto itself. Funds used to support terrorism may originate from legitimate sources, criminal activities, or both.

2.3 WHAT IS PROLIFERATION AND PROLIFERATION FINANCING?

Proliferation is the manufacture, acquisition, possession, developing, export, transhipment, brokering, transport, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legilimate purposes), in contravention of national laws, or where applicable, international obligations. It includes technology, goods, software, services and expertise.

Profliferation financing is the act of providing funds or financial services which are used, in whole or in part, to make proliferation possible. In other words, it is the financing of the proliferation activities.

While this manual speaks of Money Laundering in general terms, it is important that staff be aware that proliferation and proliferation financing may present itself in a manner similar to that of money laundering or by some other means unique unto itself. Unlike money laundering, which is concered about funds raised by illegitimate means, the source of funds used to finance proliferation can be both legal and illegal. The destination or use of those funds is for advancing the ambitions of sanction states. In many cases, the financing source is from a state or a person acting as an indirect agent of the state. As such, while some risk indicators and control elements might overlap for money laundering and proliferation financing, proliferation financing also has its own unique risk indicators.

2.4 TOKEN ISSUER AML/CFT RISKS AND VULNERABILITIES

Convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and terrorist financing abuse for many reasons. First, they may allow greater anonymity than traditional noncash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.

Virtual currency's global reach likewise increases its potential AML/CFT risks. Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border

payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems. And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible virtual currencies allowing anonymous person-to person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

Accordingly, those individuals desiring to launder criminal proceeds often turn to cryptographic tokens and other crypto currencies to aid them in the movement of such proceeds. The Company is at risk both as an issuer of tokens itself in return for cryptocurrencies but also as a holder of other cryptocurrencies and cryptographic tokens.

SECTION 3. BUSINESS RISK ASSESSMENT

The purpose of the business risk assessment is to:

- Identify the key risks faced by the Company in its day-to-day operations;
- Assess the likelihood of each risk affecting the Company;
- Evaluate the procedures and controls in place to mitigate these risks.

From an AML perspective, the primary risk to the Company is that it enters a business relationship (whether through the sale of its cryptographic ERC20 standard 'GOLD' tokens on the Ethereum blockchain ("Tokens"), the purchase of other cryptocurrencies and cryptographic tokens or otherwise) which results in the Company becoming involved in, or associated with, a financial crime or terrorist activity. The potential negative impact of this risk is huge both financially and operationally, and could result in reputational damage, loss of customers, regulatory actions and fines and lengthy legal proceedings.

There are many ways in which the Company could become involved in, or associated with, a financial crime including but not limited to:

1. Receiving payment from the proceeds of crime whether in the form of fiat currency or other crypto currencies;
2. Providing services to known criminals, terrorists or individuals with suspect business activities;
3. Enabling sanctioned individuals or companies to circumvent asset freezes or other sanctions by permitting the transfer of funds through the Company's platform;
4. Purchasing cryptocurrencies and other cryptographic tokens which are then essentially comingled with the proceeds of crime;
5. Failing to identify suspicious transactions;
6. Assisting with the movement of the proceeds of crime.

The Company's compliance programme contains an assessment and documentation of the risks associated with money laundering , terrorist financing and profliferation financing in its business, so as to allow the business to focus its resources where they are most needed to manage risks within its acceptance level.

3.1 ASSESSMENT[1]

In conducting a risk assement of its business, the Company has considered the elements set out in the Guidance Notes for virtual asset service providers.

A risk-based approach allows us to identify potential risks and target resources and effort where the risk is greatest and, conversely, reduce requirements where the risk is low. The Company's risk assessment records the following factors:

- The Company's customers, Token holders and business relationships;
    - These include risks associated with the types of customers that establish a business relationship with the Company. Examples of the categories of customers that may indicate a higher risk would include politically exposed persons (PEPs), sanctioned individuals or companies, customers whose nature, structure or relationship make it difficult to identify the ultimate beneficial owner of significant or controlling interests, as well as customers conducting transactions in unusual circumstances.
    - The company's primary objective is to provide a convenient means for participants to own gold bullion. Each GOLD token reflects ownership of an undivided specific interest in one gram of gold held in the Gold Reserves. Gold delivered upon the purchase of one GOLD Token will consist of one gram held by the Custodian on behalf of the GOLD token holders as Gold Reserves. The underlying gold bullion can be redeemed in increments of 1000 and GOLD Tokens can be traded for fiat or cryptocurrency dependant on the pairings available on participating exchanges. Accordingly, the Company's business could be seen as an ideal platform to enable money laundering.
    - There is a risk that individuals and companies which are subject to sanctions could seek to use the Tokens as a means of circumventing any asset freezing sanctions which are currently in place. The Company will need to ensure that all holders of Tokens or users of the platform developed by the Company are checked against the relevant lists of sanctioned individuals and companies so as to combat any such abuse.

[1] **Note:** Risk assessment to be completed and this section updated to reflect specific risks of the company and Tokens.

- The Token holders may, in fact, be proxies of sanctioned persons and companies and may in fact be holding them on behalf of individuals who are prohibited from doing so.

- The Company's products and services and the delivery channels through which it offers them;
  - These include risks associated with the types of products and services offered by the Company (i.e. the Tokens) and how such products and services are delivered to customers.
  - The Tokens and the Company's platform could be used as a means of funding terrorism or otherwise funding persons, companies or groups which are subject to sanctions.

- The geographic locations where the Company conducts its activities and the geographic locations of its customers;

- The acceptance by the Company of other cryptographic tokens or crypto currencies as a means of payment for the Tokens;

- The purchase by the Company of cryptographic tokens and crypto currencies as assets of the Company; and

- Any other relevant factors related to the Company business, its customers and the business relationships it has with them.

3.2 CONTROL MEASURES

Managing and mitigating the risks will involve:[2]

- Applying customer due diligence (CDD) measures to verify the identity of customers and any beneficial owners using the services of RapidID.
- Obtaining additional information or conducting enhanced due diligence on higher-risk customers via RapidID or by the Company directly

[2] **Note:** To be reviewed and amended to reflect specific policies and procedures adopted by the company.

    - Utilising the services of RapidID and official national and international databases to screen all customers and relationships to ensure that they are not Politically Exposed Persons or subject to sanctions
    - Screening Tokenholders upon redemption to combat potential money laundering including identifying and reporting any suspicious transactions and monitoring and controlling donations to non-governmental organisations.
    - Robust recording keeping procedures.
- Implementation of targeted financial sanctions procedures.
- Internal and SAR procedures

Each potential customer, will be considered using a risk based approach to ensure appropriate and necessary steps to obtain sufficient information is obtained regarding the customer's identity and business activities

In respect of risk from a money laundering or terrorist financing perspective, the Company operates in a very "HIGH" risk environment. Nonetheless, by the implementation of the anti-money laundering ("AML") and countering the financing of terrorism ("CFT") and proliferation procedures that the Company will adopt and implement, the Company will seek to mitigate the risks identified.

The Company will review this business risk assessment periodically to ensure it remains appropriate for the services it provides.

SECTION 4. LEGISLATION FRAMEWORK

4.1 LEGISLATION

Many countries including the Cayman Islands have enacted laws to combat money laundering, terrorist financing, proliferation and proliferation financing. Cayman Islands law imposes requirements on the Company to monitor our own activities for potential money laundering and/or terrorist financing and imposes substantial penalties for non-compliance. Our customers and employees should feel confident that the Company not only administers its business in full compliance with the law but also actively seeks to play a positive role as a good corporate citizen to further the goals behind this law.

Cayman Islands financial service providers are subject to legislation that captures all Cayman Islands entities and persons, together with industry-specific laws that are relevant to their corporate structure and chosen line of business. The Policy is adopted pursuant to and consistent with the laws and regulations of the Cayman Islands (as amended from time to time) and any relevant supervisory guidance or regulations promulgated by the Cayman Islands Monetary Authority ("CIMA")/Key elements of the legislative framework in the Cayman Islands include:

(1) Anti-Corruption Law (2019 Revision)
(2) Penal Code (2019 Revision)
(3) Proceeds of Crime Law (2020 Revision)
(4) Terrorism Law (2018 Revision)
(5) Misuse of Drugs Law (2017 Revision)
(6) Proliferation Financing (Prohibition) (2017 Revision)
(7) Anti-Money Laundering Regulations (2020 Revision)
(8) International Targeted Financial Sanctions and Orders
(9) CIMA Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (5 June 2020)

Severe penalties are imposed on anyone who fails to comply with the relevant policies, procedures and controls or fails to report any knowledge, belief or suspicion that another person is engaged in criminal conduct or involved in assisting or facilitating the laundering of money. It is therefore vital that all employees fully understand and comply with their legal responsibilities.

4.2 THE SPECIFIC OFFENCES UNDER THE PROCEEDS OF CRIME LAW

The POCL applies to all persons in the Cayman Islands. The three main money laundering offences are:

(a) Conceal, disguise, convert, transfer or remove (from the Cayman Islands) criminal property;

(b) Become concerned in an arrangement knowing or suspecting it facilitates the acquisition, retention, use or control of criminal property; or

(c) Acquire, use or possess criminal property

It is also an offence to attempt, conspire, incite, aid, abet, counsel or procure the commission of one of the three main money laundering offences.

The three main money laundering offences are punishable on conviction by 14 years imprisonment and/or an unlimited fine.

The term "criminal conduct" includes any conduct, wherever it takes place, that would constitute a criminal offence, if committed in the Cayman Islands. This includes drug trafficking offences, theft and fraud, robbery, counterfeiting, illegal deposit taking, blackmail and extortion. However, neither the primary legislation nor the Regulations impose a duty to look into the criminal law of any other country in which the criminal conduct may have occurred.

(d) Tipping Off

It is an offence for any person to disclose to any other person information or any other matter which is likely to prejudice any investigation or potential investigation. This is known as the offence of "tipping off".

The penalty for tipping off is a maximum of 5 years imprisonment and/or a fine.

FAILING TO REPORT

There are two offences for failing to report. The first applies to all employees of any business being conducted within the Cayman Islands and the second applies to Nominated Officers. A Nominated Officer is a person nominated by the Company for the purpose of receiving reports related to criminal conduct. This person may also be referred to as the Money Laundering Reporting Officer or MLRO. A report that is made by an employee to the MLRO, or a report filed to the Financial Reporting Authority by the MLRO, is known as a required disclosure.

(e) Failure to Disclose (Employees)

A person commits an offence if he knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in criminal conduct and he does not make the required disclosure to a nominated officer (MLRO) or the Financial Reporting Authority as soon as is practicable.
The law protects employees against legal action for breach of confidentiality in cases where the employee reports a suspicion that a person may be engaged in criminal conduct if the employee acts in accordance with the relevant procedures.

The penalty for this offence is a maximum of 5 years imprisonment and/or a fine.

(f) Failure to Disclose (Nominated Officer)

A nominated officer commits an offence if he or she knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in criminal conduct, or he has received information as a result of a disclosure made to him that gives reasonable grounds for such knowledge or suspicious and he does not make the required disclosure to the Financial Reporting Authority.

The penalty for this offence is a maximum of 5 years imprisonment and/or a fine

4.3 THE SPECIFIC OFFENCES UNDER THE ANTI-CORRUPTION LAW ("ACL")

The ACL, which initially came into effect on January 1, 2010 and has since been amended, criminalizes actions by private sector individuals and corporations, as well as public officials. Under the ACL, it is unlawful for a person to bribe either a public officer of the Cayman government, a member of the Legislative Assembly or a foreign (non-Cayman) public official in order to obtain or retain an advantage in the course of business, directly or indirectly.

Similarly, the ACL prohibits public officers of members of the Legislative Assembly of the Cayman Islands from soliciting, accepting, or agreeing to accept or obtain an improper payment for such purposes. It also criminalizes attempting, conspiring, inciting, aiding, abetting, counseling or procuring the commission of a corruption offense.

The specific offences under the ACL are:

(a) Bribery of local and foreign officials (i.e. person who directly or indirectly gives to a public officer or any public officer soliciting, accepting or obtaining, or agreeing to accept or obtain, for themselves or another person, any loan, reward, advantage or benefit with intent to interfere with administration of justice, procure or facilitate commission of an offence or protect from detection or punishment an offender)

(b) Fraud on the Government

(c) Abuses of Public or Elected Offices

(d) Secret Commissions

(e) Reporting offences (i.e. failure to report to the Commission by the person from whom a benefit was solicited or obtained and false statements to the Commission where such statements are known to be false or intended to mislead or is not consistent with a prior statement made under any law)

(f) Attempt, conspiracy or incitement to commit corruption

(g) Aiding, abetting, counseling or procuring commission of corruption

(h) Offence committed with consent, connivance or neglect of an officer

The territoriality of the ACL is far-reaching. The ACL applies to conduct committed wholly or partly within the Cayman Islands and conduct committed wholly outside Cayman and the alleged offender is a status

holders, residents and bodies corporate incorporated under Cayman Islands law (i.e. foreign acts of corruption by Cayman companies).

4.4 THE ANTI-MONEY LAUNDERING REGULATIONS

The Anti-Money laundering Regulations (2020 Revision) ("AMLR") require anyone engaged in relevant business activities to have in place systems and training to detect and prevent money laundering.

In effect, the AMLR require the Company to:

a) Maintain risk based, internal policies, procedures and controls. These procedures will include:
   i. procedures for the determination of the true identity of the applicant for business;
   ii. procedures of internal control and communication as may be appropriate for the ongoing monitoring of business relationships or a one-off transaction;
   iii. procedures to assist in the recognition and reporting of suspicious activities;
   iv. the retention and maintenance of records for the prescribed period of time;
   v. procedures to screen employees to ensure high standards of hiring;
   vi. adequate systems to identify risk as it relates to persons, countries and activities which must include checks against all applicable sanctions lists;
   vii. risk-management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.
b) Appoint a Anti-Money Laundering Compliance Officer at management level with the responsibility for monitoring and ensuring internal compliance with the Laws
c) Undertake an Internal Audit Programme
d) Ensure that there is a Staff AML training programme

The procedures contained in this manual satisfy the above requirements. They are also known collectively as Know Your Customer ("KYC") or Customer Due Diligence ("CDD") procedures. Breach of these procedures may expose the Company to regulatory enquiries and exposes individuals (Directors, officers and staff), to prosecution.

4.5 RELEVANT FINANCIAL BUSINESS

The AMLR must be followed by any person conducting "relevant financial business" (“RFB”). The conduct of which brings a person (a financial services provider or FSP) within the scope of the AML Regulations, comprises (amongst others) business that are regulated in Cayman, such as banking business, trust business, corporate/fiduciary services, securities investment business, and regulated funds business.

RFB also includes non-regulated activities that are listed in Schedule 6 of the POCL. It is within this area of non-regulated activities that the Company may find itself covered by the anti-money laundering regime.

4.5 ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

In order to meet compliance requirements, set out in the AMLR, the Company has appointed an Anti-Money Laundering Compliance Officer (“AMLCO”). Senior management is responsible for the Company’s global compliance program with all international and local legal and regulatory requirements applicable to the Company. Senior management is responsible for the oversight, selection and monitoring of the AMLCO. The Company relies on the AMLCO, under the supervision of senior management, for the following:

- Developing and maintaining systems and controls (including documented policies and procedures) in line with evolving requirements;
- Ensures regular audits of the AML/CFT programmes;
- Advises the Board of AML/CFT compliance issues that need to be brought to its attention;
- Reports periodically, as appropriate, to the Company’s systems and controls.

At publication of this manual, the AMLCO is Dean Lynnee.

4.6 OFFENCES UNDER THE REGULATIONS

If it is determined by the authorities that a financial service provider is not maintaining their anti-money laundering procedures in accordance with the Regulations, they may be guilty of an offence and liable either on conviction to a fine or a term of imprisonment for up to 2 years.

Obviously, in light of these legal and regulatory requirements, it is not only the reputation or financial risk to the Company that shall be considered, but also the more personal risk if an employee of the Company is alleged or found to have been involved in criminal conduct or is aware of such activity but neglects to report it in accordance with these procedures.

4.7 THE GUIDANCE NOTES

In order to assist financial service providers with interpretation and compliance with anti-money laundering legislation, CIMA issued its Guidance Notes on the Prevention and Detection of Money Laundering and Terrorist Financing in the Cayman Islands (the "Guidance Notes").

Although the Guidance Notes are not mandatory and go beyond the requirements of the legislation, CIMA expects financial service providers to take full and comprehensive advantage of its advice, follow its guidance and operate in accordance with the spirit and letter of the ultimate intentions of the Guidance Notes. The Guidance Notes were created as a minimum standard to be achieved by financial service providers for their operations, which may be exceeded whenever practical and appropriate.

4.8 THE TERRORISM LAW

This law contains numerous offences, penalties and defenses associated with terrorist-related activities, the handling of terrorist property and the financing of terrorism.

4.9 PROLIFERATION AND FINANCING LAW

The Proliferation Financing (Prohibition) Law, 2017 makes it an offence for any person to provide funds and economic resources to fund unauthorised proliferation activites, or to enter into or become

concerned in an arrangement which that person knows or suspects facilitates the acquisition, retention, use or control of funds and economic resources to fund unauthorised proliferation activites.

The United Kingdom has extended UN resolutions to the Cayman Islands via overseas territories Orders. These include:

(i) Iran (Restrictive Measures) (Overseas Territorites) Order 2012

(ii) North Korea (UN Measures) (Overseas Territories) Order 2006

(iii) UN Security Council Resolution 1540 which seeks to prevent non-State actors from obtaining weapons of mass destruction

SECTION 5. KNOW YOUR CUSTOMER OBLIGATIONS

5.1 INTRODUCTION

The terms KYC and due diligence are used in relation to anti-money laundering and both are used globally to describe customer identification and verification procedures, which comprise the obligations of Cayman Islands financial services providers. Collectively and for the purposes described in this manual, both of these terms encompass the various elements and stages that are required for taking on new customers and reviewing existing customers.

A general overview of the KYC due diligence requirements are set forth in this manual. In implementing the KYC requirements, the Company will prepare client onboarding forms and checklists that will include where reasonably possible the recommendations set forth in the Guidance Notes, Part IX, Sector Special Guidance for Virtual Asset Service Providers.

5.2 CUSTOMER IDENTITY

Cayman Islands legislation requires that financial service providers ensure that it is clear to whom services are being ultimately provided and take 'reasonable measures' to verify the identity of all customers.

Within the legislation, regulations and this manual, the customer may be referred to as the 'applicant for business'. CDD procedures are required for all 'applicants for business', who may be one or more of the following:

- The direct customer;
- The ultimate customer;
- The beneficial owner of the ultimate customer;
- An intermediary acting on behalf of the ultimate customer.

The customer relationship must be reviewed very carefully, and it must be established for whom CDD procedures are required, which may be more than one individual or entity. Any ambiguity or concerns should be referred to senior management and/or the AMLCO/MLRO.

5.3 CUSTOMER IDENTIFICATION PROCEDURES

When considering entering into a business relationship, there are a number of issues that encompass CDD:

- Establish the identity of the customer;
- Verify the identity of the customer and ensure that the customer is who they claim to be;
- Identify who may have control of a corporate body, legal entity or exercise control over financial resources of the customer;
- Understand the source of funds/assets/wealth which will be held, transferred or controlled by the customer including, without limitation, where the funds being transferred are the Ethereum, Bitcoin of any other cryptocurrency;
- Obtain sufficient information on the nature of the business to understand the past and future activity of the customer, together with any expected or predicted pattern of future activity.

5.4 CUSTOMER DOCUMENTATION REQUIREMENTS AND REPORTING

Knowing Your Customer ("KYC") is essential in the fight against money laundering. The Company should be satisfied that the Applicant for Business ("AFB") is who he or she claims to be as well as ensuring that sufficient information is gathered on the nature of the business that the Applicant for Business expects to undertake and any expected pattern of business.

In order to setup a new customer account to purchase the Tokens, a potential customer of the Company will be required to take the following steps to satisfy the Company's AML and KYC procedures:

1. Obtain a certified copy of government issued photo identification and proof of address. If possible the original documentation should be sighted in a face to face meeting. These items can be in the form of a driver's license or passport as well as a utility bill, rental agreement, residential contract or government letter.
2. Conduct relevant screening checks through RAPID ID and OFAC to establish: identification, Politically Exposed Persons, applicable sanctions lists, Specially Designated Nationals and Blocked Persons List.
3. Asign a risk level based on circumstance and hits on database screening.

As any problems encountered in relation to money laundering or criminal conduct are perhaps more likely to occur in the future when it might be difficult to remember what action was taken, it is essential that documentary evidence and records are properly maintained. Subject to any exemptions or exceptions, which may apply, a separate customer KYC file will contain all the information and documentation referred to in this manual.

5.5 WHEN MUST IDENTITY BE VERIFIED?

It is best practice that identity and/or ownership should be confirmed before a business relationship is established. There will be instances where it will not always be feasible to verify proposed customers prior to establishing a business relationship. There may be sound reasons which merit on-boarding a customer before verification is completed. In such instances, the Company must ensure that verification occurs as soon as is practical (or at least within 30 days), that delaying verification is necessary to avoid interrupting the normal course of business, and that through use of a risk based approach, the ML/TF risks are properly managed.

Where a customer fails to provide adequate documentation, consideration should be given to terminate the relationship and whether a suspicious activity report should be filed.

5.6 DOCUMENTATION VERIFICATION

Wherever possible, documents received should be independently verified to establish their authenticity and legitimacy.

All documents should be valid and current and if a document contains an expiry date, such as a passport, checks should be made to ensure that the expiry date has not passed. Documents that expire in the future should be renewed whenever the opportunity presents itself. However, in instances where there is sufficient information to indicate that the identification of the customer can readily be verified by other means (such as recent internet information) and the risk assessment is not high, it may not be necessary to update expired documentation. A file note should be made reflecting the justification for such decision.

Passports and other documentary evidence should appear familiar and look and feel like other comparable documents received from other customers. In the event that a document gives rise to concerns to its authenticity, referral should be made immediately to senior management and/or the AMLCO.

It should be noted that criminals will forge documents, which may not be readily obvious as fraudulent. To the extent possible, staff are expected to use their best judgement and take reasonable measure to establish that documents are recognizable and appear to be legitimate.

A common sense and risk-based approach should be taken in relation to due diligence documentation as individuals from some countries might find it difficult to provide documents that exactly match these requirements. In the event of issues arising in relation to identification documentation, refer to the Guidance Notes for further advice.

5.7 DOCUMENTATION CERTIFICATION

Whenever possible, personnel should have sight of the original due diligence documentation and verify in a face-to-face meeting. Once it is believed that the document provides adequate confirmation of identity or sufficient information, photocopies of the original should be taken. The individual who had sight of the document should complete an appropriate certification upon the photocopy as evidence that the original was seen.

The certification should contain:

- Name of certifier;
- Signature of certifier
- Capacity or job title of certifier;
- Indication that the certifier is a company employee;
- Date certified.

Whenever copy documents are received that are already certified, the Company personnel should endeavor to ascertain the identity and capacity of the certifier, if it is not readily apparent. In addition to the information required from the Company certifiers, the address and telephone number of the certifier should be obtained whenever possible.

The Guidance Notes Section 'Certification of Identification Documents' contains examples of who may be viewed as a suitable certifier and provides advice relating to the authenticity of the certification.

5.8 RISK-BASED APPROACH

It is important that the Company's principals and personnel adopt and implement the policies contained in this manual. However, it is recognized that a prescriptive approach in certain circumstances might prevent financial service providers from engaging in some legitimate businesses.

A risk-based approach is one of the most effective ways to protect against money laundering. It is essential to understand that certain risks associated with the various elements of a customer profile may be indicative of potential criminal activity, such as geographic and jurisdictional issues, business and product types, distribution channels and prevailing transaction types and amounts.

Customers will be reviewed, assessed and allocated with an appropriate level of risk of money laundering. Customers will be designated as High, Medium or Low risk.

- **High** risk customer will be subject to enhanced levels of due diligence that go beyond the core policies and principals contained in this manual;
- **Medium** risk customers will be subject to the core policies and procedures contained within this manual;
- **Low risk** customer may be subject to certain flexibility within the policies and procedures contained within this manual, however, great care should be exercised to ensure that the Company continues to meet its legal obligations.

Although it is accepted that failure to provide satisfactory due diligence documentation might be indicative of a money laundering concern, it is also recognized that due to the geographic diversity of financial businesses, on occasion it might prove difficult or impossible to obtain documentation that exactly meets the criteria set out in this manual.

If this situation should occur, and there are no reasons to suspect money laundering, the customer documentation should be referred to senior management and/or the AMLCO, together with an

explanation as to the sort of issues that arose. Senior management, in consulation with the AMLCO, will review the documentation and consider the risks associated with acceptance of identification evidence that falls outside these procedures, thereafter, providing personnel with advice and guidance as appropriate. The risks considered in the assessment and decision process, and the conclusions reached should be properly documented for the customer KYC file, with appropriate sign-off by the individuals involved. Only senior management, in consulation with the AMLCO or the MLRO, may determine the High-risk level to be attributed to any particular customer or and approve documentation that does not meet the exact requirements of the Company's anti-money laundering policy.

All customers are subject to a risk assessment in order that likely future monitoring levels are anticipated and reasonable. Risk ratings will be recorded in the file. Due diligence requirements and future planned monitoring must be commensurate with the risk level associated with the customer and enhanced due diligence will be necessary for all higher risk customers.

5.9 DATABASE SCREENING

The Company will utilise a highly structured intelligence database that contains the names of known criminals such as money launderers, terrorists, fraudsters, persons recorded on governmental 'black lists' etc. together with country profiles of jurisdictions known for high levels of criminal activity. Additionally, such databases contain the names of Politically Exposed Persons (PEPs), further details for which can be found in the following sections of this manual.

The Company will screen each new customer (all relevant parties) against a recognised database as part of the identification process at the time the request for services is received and periodically thereafter. Through this database, all customers will be screened against applicable sanction lists to ensure that business is not conducted with countries affected by sanctions imposed by the EU (European Union) UN (United Nations) or OFAC (Office of Foreign Assets Control) which includes the List of Specially Designated Nationals (SDN) and Blocked Persons List.

Further action required will be dependent upon the screening results, however senior management and/or the AMLCO, will need to be made aware of any 'hits' on the database which prompt consideration for designating the customer as high risk.

5.10 HIGH RISK CUSTOMERS

A High-Risk Customer will be one who presents a higher than normal adverse risk of involvement in money laundering or generates issues relating to money laundering requirements or any other matter that senior management or the AMLCO AMLCO consider to be significant.

In order to mitigate the risks associated with High Risk Customers, it will be necessary to consider the application of a level of enhanced due diligence for those customers in terms of initial approval and ongoing monitoring. Senior management, in consultation with the AMLCO, will determine whether the level of risk is acceptable.

Enhanced Due Diligence ("EDD") will need to go beyond the normal requirements applied to the approval and monitoring of customers, as contained within this manual. As the reasons for designation as high risk will vary from customer to customer, the nature and level of enhancement will need to be determined separately as and when high risk customers are identified, and procedures will need to explain how the increased risks will be minimized.

Should it be determined that a customer who fulfils the criteria for designation as high risk does not warrant enhanced due diligence, the reasons for the decision and the manner in which the risks are mitigated, should still be fully documented and placed upon the customers' file.

In addition, any EDD procedures carried out during the approval process, together with proposed procedures for future monitoring, should be fully documented and placed upon the customer file. In the event that any problems are encountered in the future when personnel may not readily recall the steps that were taken, the Company will be in a position to supply evidence of the due diligence that was carried out at the time and provide the rationale for proposed ongoing monitoring.

International best practice recommends that special attention should be applied to the following issues:

- High risk countries;
- Politically exposed persons ("PEPs");
- Businesses attractive or susceptible to money laundering.

All High-Risk Relationships will be recorded for the purposes of reporting and monitoring.

5.11 HIGH RISK AND NON-COMPLIANT COUNTRIES

Certain countries are associated with predicate money laundering crimes such as drug trafficking, fraud and corruption and consequently pose a higher potential risk to the Company. Conducting a business relationship with persons from such a country may expose the Company to greater reputational risk and legal risk.

Particular attention should be given to countries:

- without effective or equivalent anti-money laundering strategies;
- where cash is the prevailing and normal medium of exchange;
- political instability and/or high levels of public or private sector corruption;
- known drug transit or drug trafficking countries.

The Company will consult publicly available databases or any lists published by CIMA and establish whether customer connections with the listed countries warrant assessing the customer as high risk. Consideration should be given to the manner in which any prevailing risks may be able to be mitigated by conducting additional and more detailed due diligence. Caution should be exercised when accepting identification documentation, particularly certified copy documentation, from high-risk or non-compliant countries.

5.12 POLITICALLY EXPOSED PERSONS ("PEPs")

A Politically Exposed Person or PEP is a term that is used to describe a person who holds a public position that may be exposed to corruption. The following list contains examples of persons who may be considered PEPs, although this list should not be viewed as exhaustive:

- Head of State;
- Government Ministers and Politicians;
- Influential public officials;
- Judges;
- Military commanders and high-ranking military officials;
- Family members or close associates of any of the above;
- Business partners or corporate connections of any of the above.

Adverse risk is created for PEPs as they might use their public position, or find that their public position is unknowingly used, for their own personal benefit or the benefit of others who may be involved in illegal activities such as corruption, bribery and fraud.

PEPs present considerable reputational risk to a financial service provider if that institution is found to be involved with public official who abuses his/her position. Adverse risk is increased considerably when a PEP is located in a high-risk country.

The Company will ensure that each underlying beneficial owner or controller is not a PEP by performing searches on official national and international databases to screen names against its database or referring to publicly available information. The results of such verification will be recorded. In the event that a PEP is identified, the Company will:

a. Assign a rating of high risk to the customer;
b. Complete PEP Report, ensuring Senior Management and the board of directors approves establishing a business with the customer;
c. Conduct enhanced due diligence and be vigilant in monitoring the business relationship;
d. Ensure reasonable measures will be taken to establish source of wealth and source of funds;
e. PEP relationships will be tracked in View Point for the purposes of reporting and monitoring

5.13 SANCTIONED INDIVIDUALS/ENTITIES

When considering accepting new customers, care must be taken to ensure that the Company is not conducting business with countries affected by sanctions imposed by the EU (European Union) UN (United Nations) or OFAC (Office of Foreign Assets Control) as a result of accepting that new business.

Pursuant to the Proceeds of Crime Law, the Anti-Money Laundering Regulations and the Terrorism Law the Company must file a Suspicious Activity Report to the Financial Reporting Authority if a relationship is discovered that contravenes a sanctions order or a direction under the Proliferation Financing (Prohibition) Law.

The Company shall document and record all the actions that were taken to comply with the sanctions regime and the rationale for such action. Senior management, in consultation with the AMCLO, will consider if any further action is required such as freezing funds and/or informing the authorities as required under relevant laws.

All individuals/entities identified on any sanction list will be recorded for the purposes of reporting and monitoring.

5.14 ENHANCED DUE DILIGENCE

EDD will need to go beyond the normal requirements applied to the approval and monitoring of customers, as contained within this manual. EDD is an iterative, risk-based exercise - the higher the level of potential risk, the greater the corresponding level of due diligence. EDD is a multi-tiered process; the steps taken vary depending upon the information obtained through the process. In general, if relevant adverse information is identified in one phase, the EDD activity must continue to the next level. If nothing is found as a result of the EDD investigation and review, EDD can be considered complete. It is not possible to prescribe a detailed process for each EDD investigation, as each one will be different. In all cases, EDD investigations should be logical, methodical and properly documented.

In the event that any problems are encountered in the future when personnel may not readily recall the steps that were taken, the Company will be in a position to supply evidence of the due diligence that was carried out at the time and provide the rationale for proposed ongoing monitoring. For completeness, all negative results pertaining to EDD that has been performed should also be documented in the compliance file.

EDD must be conducted on all customers who are identified as a PEP or designated as High Risk.

5.15 ONGOING MONITORING

Once customer identification procedures are fulfilled and the customer is accepted, it will still be necessary to ensure that due diligence documentation continues to remain appropriate. In addition, it is essential to ensure that ongoing activity, if any, is consistent with the future plans and expectations that were advised at the outset of the relationship.

The frequency and nature of the monitoring will depend upon the type of business and the risk level associated with a particular customer. Further details relating to risk assessments and monitoring are provided later in this manual. The scope, outcome and recommendations of the monitoring process should be documented and placed upon the relevant customer file.

5.26 DECLINED & CLOSED BUSINESS

The obligation to report suspicious activities extends to declined business. Business may be declined because we have concerns regarding the bona fides of underlying parties to be involved or the transactions they wish to under-take. In situations where such concerns are arise, the situation must immediately be referred to a member of senior and/or the AMLCO and where the decision is made to decline the business, consideration must be given to the filing an Internal Report.

In all circumstances where business is declined as a result of such concerns a Declined Business Report must be completed and passed to the AMLCO who will maintain a Register of Declined Business.

SECTION 6. IDENTIFICATION PROCEDURES

6.1 IDENTIFICATION & VERIFICATION PROCESS

An Applicant for Business is the person or entity (e.g. company, partnership, trust or unincorporated association) whose identity must be verified. In general, this will include, any individual customer, any company or other entity that is to become our customer, the principal shareholders of a customer company, the relevant partners in respect of a partnership, settler and potentially the beneficiaries in respect of a trust.

It may also include any individual who gives instructions to the Company or where an individual is a signatory on a bank account or acts under a power of attorney. Detailed guidance is provided below in respect of all situations.

There are certain exceptions permitted by law as it relates to the collection and verification of KYC documentation. These exceptions are known as Simplified Due Diligence (SDD) and are discussed later in this Section.

Regardless of how the process is triggered, the identity of the following persons must be verified in accordance with our verification process.

- Each individual who will ultimately beneficially own, or be beneficially entitled to, on a look-through basis, 10% or more of a company or entity which is a holder of Tokens;
- Directors of a company or entity (if multiple directors, the risk assessment will determine how many Directors should be verified) which is a holder of Tokens;
- Any person authorized to give instructions, a signatory, or holds Power of Attorney;
- The general partners of a partnership, regardless of the percentage of their interest;
- Settlors or Contributors of capital (whether named or otherwise);
- The manager of a mutual fund
- Trustees, Beneficiaries, Protectors and Enforcers of a Trust.

The customer relationship must be reviewed very carefully, and it must be established for whom KYC procedures are required, which may be more than one individual or entity. Any ambiguity or concerns should be referred to senior management and the AMLCO.

6.2 CUSTOMER VERIFICATION [3]

The following documentation must be obtained to verify customers:

6.2.1 INDIVIDUALS/DIRECTORS/OFFICERS (may be more than one)

1. The following information is required for all *individual* customers:

   - Full name/names used;
   - Correct permanent address including postcode (if appropriate);
   - Date and place of birth;
   - Nationality;
   - Occupation;
   - Purpose/nature of the intended business;
   - The source of funds (i.e., generated from a transaction or business).

2. Photo Identification: Obtain one certified or notarized copy of a document that establishes the identity of the person. This may include:
   - Passport
   - Photo Driver's License with signature
   - Armed Forces ID
   - Other Government issued identification

3. Proof of Address: Obtain one certified or notarized copy of a document that establishes the residential address of the person. This may include:

   - Recent utilities bill (not more than three months old)
   - Reference from respected professional [4] who knows the customer
   - Copy of contract of employment or banker's or employer's written confirmation

[3] **Note**: To be reviewed/amended to reflect the specific procedure being adopted.
[4] *lawyer, accountant, priest, teacher, director of regulated institution*

4. Reference Letters- A professional reference may be required for individuals with a 10% or greater shareholding or beneficial ownership and all directors. A reference letter is not required in situations where SDD is appropriate.

   Where directors are acting as such by virtue of their employment with a corporate customer and KYC on that corporate has been satisfied, evidence of employment is accepted in place of the reference.

   All reference letters should be addressed to the Company.

6.2.2 CORPORATE CUSTOMERS

The following corporate records will also comprise due diligence documentation for a company:

- Certificate of Incorporation;
- Certificate of Name Change, if any;
- Certificate of Good Standing (dated within prior 6 months), if an existing entity;
- Name and address of Registered Office, if not the Company;
- Name and address of any other place of business;
- Register of Members/Shareholders;
- Register of Directors and Officers;
- Powers of Attorney, if any;
- Memorandum & Articles of Association;
- Board of Directors Resolution approving entering the relationship with the Company.

6.2.3 PARTNERSHIPS & UN-INCORPORATED CUSTOMERS

The core policies for corporate customers should also be followed for partnerships and un-incorporated customers. The following documentary evidence comprises the due diligence required for all un-incorporated entities:

- Certificate of Registration;
- Partnership Agreement;

- If not indicated in the Partnership Agreement, confirmation of the business or trading address of the Partnership;
- Where the Partnership has Officers and/or Managers, a list of the Officers and/or Managers;
- Identification evidence for at least two partners, one of which must be an General Partner;
- Identification evidence for each Limited Partner holding 10% or more of the total limited partnership interests in the Partnership;
- Identification evidence and confirmation of the relationship to the company for all authorized signatories, including powers of attorney, if different to above;
- Identification evidence for anyone who is authorized to control the company (officers/managers) in any way or is authorized to give instructions.

6.3 SIMPLIFIED DUE DILIGENCE

As a rule, the Company will obtain full due diligence for all customers in the manner described in the previous sections of this manual. However, there are circumstances when obtaining such evidence may be unnecessary duplication, commercially onerous and of no real assistance in the prevention of money laundering.

Where a customer relationship has been identified as a lower risk, Simplified Due Diligence ("SDD") can be applied. SDD shall not be applied to any business relationship or one-off transaction believed to present a higher risk of money laundering or terrorist financing. Any assessment of lower risk must be consistent with the findings of CIMA or any risk assessment carried out by the Cayman Islands Anti-Money Laundering Steering Group.

SECTION 7. MONITORING

7.1 MONITORING REQUIREMENTS

Once identification procedures are complete and the Company has established a relationship with the customer, the Company must continue to monitor customer structure and any activity, if apparent, to ensure that it is consistent with expectations and to ensure that due diligence documentation remains up to date and in keeping with current requirements. The frequency and nature of the monitoring processes will depend upon the type of customer, the business undertaken, and the risk rating assigned to the customer.

7.2 MONITORING AREAS

The types of issues that should be reviewed include:

- Transactions upon redemption of the Tokens and the intended recipients;
- Changes in customer structure, business relationships etc.;
- Changes in individuals including directors, officers, authorized persons etc.;
- Jurisdictions within which the customer is based or conducts business;
- Expectations were achieved;
- Any issues considered unusual.

The rationale for any changes in structure or expectations should be reviewed and investigated until an acceptable level of satisfaction is achieved. If full satisfaction cannot be achieved, the customer should be subjected to enhanced due diligence procedures, which might include increasing the frequency of the customers' monitoring process.

7.3 PERIODIC REVIEWS

The Company shall periodically conduct a review of CDD information, activity and transactions, and internet searches (collectively, the "Periodic Review") for all customers. The frequency of the review will be based on the Risk Assessment: High Risk Customers will be reviewed annually; Medium Risk Customers every 2 years and Low Risk Customers will be reviewed every three years. The objective of the Periodic Review is:

- ensure that customer activity conforms with the stated information at the time the relationship was established. (i.e. license status, volume of activity, etc.)

- ensure that due diligence documentation remains appropriate
- ensure risk rating remains appropriate

The findings of the periodic review will be documented for each entity and placed in the customer files.

SECTION 8. RECORD KEEPING

8.1 RECORD KEEPING REQUIREMENTS

The Company is required to retain records concerning customer identification and transactions and other records that pertain to anti-money laundering procedures.

Due diligence documentation might include:

- Identification evidence;
- Any other due diligence collected during customer take-on and monitoring;
- Financial transaction details and statements;
- File notes, minutes and other records relating to customer activity
- New business approval records including, due diligence checklists and any supporting documentation.

In addition, the following records should be retained:

- Training registers, testing records and plans;
- Suspicious Activity Reports ("SAR") and accompanying documentation;
- Register of Enquiries containing enquires made to, or received from, the FRA;
- Compliance & MLRO monitoring records.

The Company will ensure adequate safeguards are in place on the confidentiality and the use of information exchanged when sharing information required for due diligence and AML/CFT risk management within the group of companies.

8.2 RECORD RETENTION PERIOD

Records must be retained for a minimum of 8 years from the date of closure of the customer or following the end of a money laundering investigation, if any.

8.3 DESTRUCTION OF RECORDS

Personnel should refer to senior management prior to destroying any customer records. Records may not be destroyed unless written approval is received from senior management, who will confirm the name of customer, the nature of the records to be destroyed and the relevant dates (e.g. date of closure and permitted date of destruction).

The MLRO will ascertain whether any money laundering investigation is in progress or was ever in progress. The MLRO will give approval for the destruction of the records if no SAR was filed and if there is no ongoing money laundering investigation in the past 5 years.

If the MLRO is called upon to approve the destruction of records for a customer for whom a SAR was filed, enquiry should be made to the Financial Reporting Authority ("FRA") to ensure that the records are no longer required.

If a money laundering investigation is ongoing and/or the FRA does not give approval for destruction of the records, it will be prudent for the MLRO to arrange for the secure and confidential storage of all relevant customer records separate from other customer records.

It is essential that all documentation, including checks and approval authorities, relating to the destruction of records should be documented and retained on file. Any FRA confirmation should also be received in writing and placed upon the SAR reporting file.

SECTION 9. TRAINING

9.1 INDUCTION AML TRAINING

As part of the induction training, all new employees will receive anti-money laundering training. Permanent and temporary employees should be trained in the same way, while taking account the scope of work that might be allocated to a temporary employee.

New employees should be interviewed to ascertain current level of understanding of money laundering. As a minimum, new employees should be provided with:

- Access to the Company's Anti-Money Laundering Compliance Manual;
- Explanation of an individual's anti-money laundering obligations;
- Identity and location of the MLRO and DMLRO;
- Location of a blank internal SAR.

A detailed explanation of the circumstances that might lead to the necessity to file an internal suspicious activity report ("SAR") must be provided. The identity and location of the MLRO and DMLRO and whereabouts of a blank internal SAR must also be provided, in order to enable any new employee to file an internal SAR if needed.

All new employees must also be advised of the confidentiality afforded to any SAR and relevant documentation to ensure that they do not compromise their own confidentiality or jeopardize the integrity of customer records.

9.2 REQUIRED ANNUAL AML TRAINING

All staff are expected to attend an anti-money laundering training at least once annually. All employees that attend these annual AML trainings are expected to produce evidence of completion of training by way of a a certificate or copy of registration to the AMLCO as evidence that the individuals attended. Therefore, all personnel, regardless of seniority level will be required to participate in an AML training session at least once a year.

9.3 ADVANCED TRAINING

The AMLCO/MLRO, Directors and Senior Management are required to have a more in-depth training on all aspects of anti-money laundering. In addition, the AMLCO and MLRO will keep abreast of current money laundering trends and Cayman Islands policies.

9.4 STAFF TRAINING RECORDS

Senior management shall maintain records which include details of the content of the training programs provided, the employees who have received the training, the date on which the training was delivered, the results of any testing.

SECTION 10. SUSPICIOUS ACTIVITY REPORTING

Principal Money Laundering Offences

The principal money laundering offences are the following offences contained in the Proceeds of Crime Law (but equivalent offences are contained in the other laws within the AML Regime):

- **Arrangements relating to criminal property**: entering into or becoming concerned in an arrangement which the person knows or suspects, facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person;

- **Possession of criminal property**: acquiring, using or having possession of criminal property;

- **Concealment of criminal property**: concealing, disguising, converting, transferring criminal property or removing it from the Cayman Islands. Note that concealing or disguising criminal property includes concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it.

- **Failing to Report a Suspicion**: a person will commit an offence if:

- he knows or suspects, or has reasonable grounds for knowing or suspecting that another person is engaged in criminal conduct;
- the information on which his knowledge or suspicion is based came to him in the course of a regulated business (or as the result of an internal report in the case of the MLRO); and
- he does not make the required disclosure to the MLRO concerning the person and property involved in the suspected criminal conduct or, in the case of the MLRO, to the FRA, as soon as practicable after the information comes to him.

- **Tipping Off:** a person commits the offence of "tipping off" if he discloses that a suspicious activity report has been made (or will be made), that a police investigation is underway (or proposed) or that access to information orders have been made or sought, and he knows this disclosure is likely to prejudice an investigation.

The criminal penalties are as follows:

- **Arrangements, Possession or Concealment of Criminal Property**: up to 14 years imprisonment and an unlimited fine.

- **Failure to Report a Suspicion**: up to 5 years imprisonment and an unlimited fine.

- **Tipping off**: up to 5 years imprisonment and an unlimited fine.

10.1 SUSPICIOUS ACTIVITY REPORTING REQUIREMENTS

It is the responsibility for everyone to identify risks of money laundering and criminal conduct, and to do so, they must know how to identify suspicious activities, which are typically the first indicator of money laundering. Further, it is the mandate of all employees to report these activities to the MLRO.

10.2 UNUSUAL & SUSPICIOUS ACTIVITY

Unusual activity is that which is not consistent with customer's known or expected activity or is abnormal for the type of customer or structure. The key to identifying unusual activity is to know enough about a particular customer and its normal activity to be in a position to recognize anything unusual. There is an important distinction between activity that is considered to be unusual and activity that is believed to be, or known to be, connected with criminal conduct, money laundering or terrorist financing.

At times the Company's personnel may come across activity or behaviour that is considered to be unusual and not consistent with expectations. Unusual activity should be investigated, in conjunction with the customer, the Company's personnel and if appropriate, the MLRO.

If the results of investigations reach a satisfactory conclusion and there is no knowledge, suspicion or reasonable grounds for suspicion of criminal conduct, then there is no requirement to file an internal SAR.

However, if investigations result in the conclusion that there is knowledge, suspicion or reasonable grounds for suspicion of criminal conduct or money laundering, then the activity is not only unusual but

is now also deemed to be suspicious. In such cases an internal SAR must be filed with the MLRO as soon as reasonably practicable.

10.3 FILING A SUSPICIOUS ACTIVITY REPORT

Staff members are required to report any suspicion of criminal conduct directly to the MLRO as soon as possible. The report must be made in writing.

Once it is determined that the activity is suspicious, no further enquiry should be made with the customer and the customer must never be advised that anyone finds their activity suspicious nor that a SAR was or will be filed.

To advise the customer of a suspicious of money laundering is known as 'tipping off, which is a criminal offence that attracts financial and prison term penalties. The MLRO will provide advice and guidance should the need arise to deal with the customer and/or respond to the customer's enquiries.

Once one SAR is filed for a particular customer, staff should be alert to any additional activity or contact with the customer. Even though additional activity might not appear to be suspicious in itself, personnel should bear in mind that the additional information might assist the FRA in their enquiries.

Therefore, an additional internal SAR will usually be filed with the MLRO for any additional activity, who will then determine whether to file again with the FRA.

Any concerns relating to suspicious activity should be referred to the MLRO immediately.

10.4 MLRO RESPONSIBILITY

Upon receipt of a SAR from any of the Company's personnel, the MLRO will:

- Sign the report and acknowledge receipt in writing to the relevant individual;
- Assess whether the SAR was filed on a timely basis;
- Place a copy of the report and receipt onto the internal SAR file;
- Assess the report and supporting evidence to determine the requisite course of action;

- Consider the Company's policy and procedures, the legislation, regulations, Guidance Notes and any other applicable developments.

If the MLRO concurs that the activity does give rise to a suspicion of money laundering, then the MLRO will:

- File an external SAR with the FRA as soon as practicable;
- Place a copy of the SAR onto the external SAR file;
- Consider whether the relationship should continue;
- Advise staff members involved how to proceed.

Depending upon the nature of the suspicious activity, the MLRO must decide whether to recommend that the business relationship continue. Consideration should also be given to conducting further investigations and/or terminating the relationship.

Care must be exercised to ensure that the customer is not alerted to the SAR or the suspicions. In serious circumstances, the MLRO may consult with senior management as to how to proceed. If it is decided that the relationship is not to continue, extreme care should be exercised in notification to the customer to ensure that he/she is not inadvertently 'tipped off' that a SAR was filed.

If the MLRO does not agree that the activity is suspicious, then the MLRO will:

- Determine the reason for the basis of that decision;
- Document the reason on the SAR or attach documentation to the SAR;
- File a further copy on the internal SAR file.

10.5 SAR RECEIPT

It is important that the individual filing the SAR does not retain any confidential information. The MLRO will acknowledge in writing receipt of a SAR from a member of staff (‘the receipt”).

The receipt should be retained with the individual's personal records indefinitely in case it is ever needed for the courts as evidence that a SAR was filed, and an individual's obligations were met. The receipt

should be considered to be an important document as it could be used as a defense to prove that an individual met his or her obligations under the anti-money laundering requirements.
The MLRO will also place a copy of the receipt on the internal SAR File.

10.6 SAR REGISTERS

A separate register will be maintained of all internal reports received from company personnel and all external reports made to the FRA by the MLRO.

In addition to a copy of each internal SAR, the internal SAR register will contain the following:

- Date of the report;
- Name of person filing the internal report;
- Name of the subject of the report (including account number if relevant);
- Reason for not filing the SAR with the FRA, if relevant.

In addition to a copy of each external SAR, the external SAR register will contain the following:

- Date of the report;
- Name of person filing the internal report;
- Name of the subject of the report (including account number if relevant);
- Reason for filing the SAR with the FRA;
- Responses from the FRA.

Care should be exercised to ensure that confidential customer information pertaining to the SAR is not included in any meeting notes or minutes that may be held to consider the matter or form part of the customer correspondence.

10.7 SAR RETENTION PERIOD

All SAR record must be kept for 5 years or until such time that the FRA advises that any money laundering investigation is concluded and confirms that records may be destroyed.

Approval from the FRA to destroy SAR records must be received in writing and placed with the external SAR records.

SECTION 11: INTERNAL AUDIT FUNCTION

It is a requirement of the Anti-Money Laundering Regulations that all financial service providers conduct an AML/CFT audit on a regular basis. Senior management is responsible to ensure that an internal audit is conducted at least once every three years.

11.1 INTERNAL AUDIT COMPONENTS

The following items will be included in the Company's AML/CFT Audit:

- attest to the overall integrity and effectiveness of the AM/CFT systems and controls;
- assess its risks and exposures with respect to size, business lines, customer base and geographic locations;
- assess the adequacy of internal policies and procedures including Customer identification and verification, Record keeping and retention, Reliance relationships and supporting documentation, and Transaction monitoring;
- test compliance with the relevant laws and regulations;
- test transactions in all areas of the Company, with emphasis on high-risk areas, products and services;
- assess employees' knowledge of the laws, regulations, guidance, and policies & procedures;
- assess the adequacy, accuracy and completeness of training programmes; and
- assess the adequacy of the Company's process of identifying suspicious activity.

SECTION 12. KNOW YOUR EMPLOYEE

Senior Management is responsible for ensuring that procedures for staff recruitment and vetting require that sufficient checks are made into a potential member of staff's background before they are taken on. The Company will conduct one or more of the following:

- verify the identity and background of the potential staff member
- review of education and work experience
- verify professional qualifications
- verify references and supporting documents
- run employee names through an AML screening database
- perform any other due diligence measures that may be necessary (i.e. internet research)

SECTION 13. ANTI CORRUPTION POLICY

The laws of most countries make the payment or offer of payment or even receipt of a bribe, kickback or other corrupt payment a crime which could subject the Company and individual employees to fines and/or imprisonment. These anti-corruption laws make it a crime to pay, offer, or give anything of value to foreign governmental officials, a foreign political party (or official thereof) or candidate for foreign office, for the purpose of influencing the acts or decisions of those officials, parties or candidates.

In 2010, the Cayman Islands introduced the Anti-Corruption Law, which established an anti-corruption body and criminalizes acts of corruption and bribery of public officers as well as a range of other offences such as frauds on the government.

The Company is committed to conducting its business with honesty and integrity and in compliance with the laws of all the countries in which the Company is active. This includes compliance with all laws, domestic and foreign, prohibiting improper payments or inducements to any person, including public officials.

13.1 STATEMENT OF POLICY

Personnel shall not permit any use of the funds or other assets of the Company for any unlawful or improper use.

Personnel shall not make, or authorize anyone to make on behalf of the Company or receive, any loan, reward, advantage or benefit payments or gifts or offers or promises to pay money or give anything of value to or for the benefit of any person, or organization, including government agencies, individual government officials, any "Public Officer" or member of the Legislative Assembly, private companies and employees of those private companies under any circumstances.

All personnel should be mindful of any unusual payment or transaction that may be seen as a bribe, purchasing influence, election fraud, breach of trust, or cash for honors. Any uncertainty or questions should be referred to the MLRO. If any personnel suspect corrupt activity, an Internal Suspicious Activity Reporting Form must be submitted to the MLRO.