Introduction

Virtual Markets Ltd is registered in St. Lucia, with company registration number 2023-00452, operating under the trading name Virtual Markets (hereinafter "The Company").

The Company has implemented policies, controls and procedures in line with the Prevention and Suspension of Money Laundering and Terrorist Financing Regulations.

Definitions

The Policy includes inter alia the Company's Internal control rules regarding the Guidelines and the Company's risk assessment policy regarding risk based approach for ML/TF risks.

The Money Laundering (ML) means the concealment of the origins of illicit funds through their introduction into the legal economic system and transactions that appear to be legitimate.

There are three recognized stages in the money laundering process: placement, which involves placing the proceeds of crime into the financial system; layering, which involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds; integration, which involves placing the laundered proceeds back into the economy to create the perception of legitimacy.

The Terrorist Financing (TF) means the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism in the meaning of applicable legislation.

Sanctions mean an essential tool of foreign policy aimed at supporting the maintenance or restoration of peace, international security, democracy and the rule of law, following human rights and international law or achieving other objectives of the United Nations Charter or the common foreign and security Policy of the European Union. Sanctions include: international sanctions which are imposed with regard to a state, territory, territorial unit, regime, organization, association, group or person by a resolution of the United Nations Security Council, a decision of the

Council of the European Union or any other legislation imposing obligations on Saint Lucia; sanctions of the Government of Saint Lucia which is a tool of foreign policy which may be imposed in addition to the objectives specified in previous clauses in order to protect the security or interests of Saint Lucia.

International Sanctions may ban the entry of a subject of an international sanction in the state, restrict international trade and international transactions, and impose other prohibitions or obligations.

The Customer means a natural person or a legal entity which has the business relationship with the Company or a natural person or legal entity with which the Company enters into the occasional transaction.

The Beneficial Owner means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or exercises control in another manner over a transaction, act, action, operation or step or over another person and in whose interests or for whose benefit or on whose account a transaction or act, action, operation or step is made. In the case of a legal entity, the beneficial owner is a natural person whose direct or indirect holding, or the sum of all direct and indirect holdings in the legal entity, exceeds 25 percent, including holdings in the form of shares or other forms of bearer.

AMLRO means Money Laundering Reporting Officer, who is appointed to the Company as a Compliance officer. The Employee means the Company's employee, including persons which are involved in application of these AML Guidelines in the Company.

The Management Board means management board of the Company.

The Business Relationship means a relationship that is established upon conclusion of a long-term contract by the Company in economic or professional activities for the purpose of provision of a service or distribution thereof in another manner or

that is not based on a long-term contract, but whereby a certain duration could be reasonably expected at the time of establishment of the contact and during which the Company repeatedly makes separate transactions in the course of economic or professional activities while providing a service.

The Occasional Transaction means the transaction performed by the Company in the course of economic or professional activities for the purpose of provision of a service or

sale of goods or distribution thereof in another manner to the Customer outside the course of an established business relationship.

Virtual currency/Crypto currency/Crypto According to FinCEN's guidance, virtual assets are considered "a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes." It includes cryptocurrencies, convertible virtual currencies (CVCs), and digital assets that rely on distributed ledger technology. This definition helps clarify how virtual assets are categorized and regulated under US laws and regulations related to anti-money laundering and counter-terrorist financing. It is advisable to refer to official guidance from FinCEN for the most accurate and up-to-date information.

In addition, a virtual assets refers to a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015,pp 35–127) or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive.

PEP(Politically Exposed Person) means PEPs). They include— *(Amended by S.I. 82/2012)*

(a) a senior official in the executive, legislative, administrative, military or judicial branches of a foreign or domestic government (whether elected or not); *(Amended by S.I. 82/2012)*
(b) a senior official of a major foreign or domestic political party; *(Amended by S.I. 82/2012)*
(c) any corporation, business or other entity formed by, or for the benefit of, a senior political figure;
(d) 'immediate family' i.e. parents, siblings, spouse, children and in-laws as well as 'close associates' (i.e. a person known to maintain unusually close relationships with PEPs).

Structure of the Management of the Company

The organizational structure of the Company must correspond to its size and the nature, scope,and the level of complexity of its activities and services provided, including the risk appetite and related risks, and must be structured in accordance with the principle of three lines of defense.

The organizational structure of the Company must correspond to the complete understanding of potential risks and their management. The reporting and subordination chains of the Company must be ensured in such a way that all employees know their place in the organizational structure and know their work duties.

The Management Board

The Management Board is the carrier of the culture of compliance with the requirements of money laundering and terrorist financing prevention, guaranteeing that the Management Board members and employees of the Company operate in an environment where they are fully aware of the requirements for the prevention of money laundering and terrorist financing and the obligations associated with these requirements, and the relevant risk considerations are taken into account to a suitable extent in the decision-making processes of the Company.

The Management Board members bear ultimate responsibility for the measures taken to prevent the use of the Company's services for money laundering or terrorist financing. They provide oversight and are accountable for: establishing and maintaining AML processes, procedures, risk, and control processes; adopting these Guidelines and other internal guidelines and instructions; determining the Company's Guidelines for AML measures; appointing an AMLRO and ensuring that the MLRO has the powers, resources and expertise required to perform their assignment; allocating sufficient resources to ensure the effective implementation of the AML Policy and other related documents and to maintain the organization; ensuring all relevant employees complete annual AML training.

The first line of defense – the Employees

The first line of defense has the function of applying the due diligence measures upon business relationship and occasional transactions and applying due diligence measures during the business relationship.

First line of defense comprises the structural units and employees of the Company with whose activities risks are associated and that must identify and assess these risks, their specific features and scope and that manage these risks by way of their ordinary activities, primarily by way of application of due diligence measures. The risks arising from the activities of and provision of services by the Company belong to the first line of defense. They are the managers (owners) of these risks and responsible for them.

The employees of the Company must act with the foresight and competence expected from them and according to the requirements set for their positions, proceeding from the interests and the goals of the Company, and ensure that the

country's financial system and economic space are not used for money laundering and terrorist financing. The Company takes measures to assess the suitability of the employees before they start working with the relevant training.

For the aforementioned reasons, the employees are required to: adhere to all requirements outlined in the Guidelines and other related documents; collect required customer information in accordance with their function and accountabilities; report information, situations, activities,transactions or attempted transactions that are unusual for any type of service or customer relationship, regardless of the amount,whether or not the transaction was completed without delay to the AMLRO; not inform or otherwise make customers aware if the customer or any other customers are or may be the subject of a report or if a report has been or may be filed; complete the appropriate AML training required for the employee's position.

The second line of defense – Compliance, AMLRO

The second line of defense consists of the risk management and compliance functions. These functions may also be performed by the same person or structural unit depending on the size of the Company and the nature, scope and level of complexity of their activities and provided services, incl. the risk appetite and risks arising from activities of the Company.

The objective of the compliance function is to guarantee that the Company complies with effective legislation, guidelines and other documents and to assess the possible effect of any changes in the legal or regulatory environment on the activities of the Company and on the compliance framework. The task of compliance is to help the first line of defense as the owners of risk to define the places where risks manifest themselves (e.g., analysis of suspicious and unusual transactions, for which compliance employees have the required professional skills,
personal qualities, etc.) and to help the first line of defense manage these risks efficiently.

The second line of defense does not engage in taking risks. It should also produce reports that should be submitted to the Board of Directors at least quarterly. A more detailed report than the one submitted to senior management, should be submitted to the Board of Directors.

Risk policy is implemented, and the risk management framework is currently controlled by the management board. Upon the growth of operations the Company will consider appointing an independent risk management function. The performer of the risk management ensures that all risks are identified, assessed, measured, monitored, and managed, and informs the appropriate units of the Company about them. The performer of the risk management function for the purposes of AML

primarily performs the supervision over adherence to risk appetite, supervision over risk tolerance, supervision over identification of changes in risks, performs the overview of associated risks, and performs other duties related to risk management.

The Management Board has appointed an AMLRO for performing the second line of defense functions. This person is not operationally involved in the areas that the MLRO will be monitoring and verifying and is thus independent in relation to these. The MLRO is accountable for the following activities:

- produce and when necessary, update the Company's Guidelines; monitoring and verifying on an ongoing basis that the Company is fulfilling the
- requirements prescribed by these Guidelines and related documents and according to
- external laws and regulations provide the Company's staff and Members of the Board with advice and support
- regarding the rules relating to money laundering and terrorist financing inform and train the members of the Management Board and relevant persons about the rules relating to money laundering and terrorist financing investigate and register sufficient data on received internal notifications and decide whether the activity can be justified or whether it is suspicious; file the relevant reports (i.e. UARs, SARs, STRs, etc.) with the appropriate regulatory authorities in accordance with local jurisdictional requirements; check and
- regularly assess whether the Company's procedures and guidelines to prevent the use of the business for money laundering or terrorist financing are fit for purpose and effective; identify the incidents in accordance with the Company's Guidelines and take measures regarding such incidents.

The AMLRO reports to the Management Board quarterly. This report must be in writing and include at least the following items: number of customers under all risk classifications, number of hits of persons in relation to the Sanctions lists and applied measures, number of customers or customers' representatives identified as PEPs or persons with a connection to a PEP, number of internal notifications on suspicious activity or transactions; number of the relevant reports (SARs, UARs, etc.) reported to the Saint Lucia Financial Intelligence Authority (FIA) through filling the form found in *Appendix I*; number and content of a request for information from the FIA within the framework of an investigation; confirmation that the Company's risk assessment for money laundering and terrorist financing is up to date; confirmation that these Guidelines and other related documents are up to date; confirmation that the staffing in respect of AML measures is sufficient; all inadequacies (if any) identified by control function have been addressed; list of obligatory trainings which have been held for the staff in respect of AML measures.

The criteria for accepting new clients

a. Completion of the Company's Registration Process (together referred to as "Identification").

b. The Company will classify Clients into various risk categories on a risk-based approach and based on the risk perception decide on the acceptance criteria for each category of Client;

c. 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.

d. All documents and data must be collected before accepting a new Client.

e. No account will be opened in anonymous or fictitious names(s);

Below are the risk categories that Clients are classified:

Low Risk Clients

The Company will accept Clients who are categorized as low risk Clients as long as the general principles above are followed. In this case simplified due diligence can be applied upon the discretion of the Company.

Low risk indicators:

(a) Those facility holders identified in regulation 103 of the Money Laundering Prevention Act as exempt e.g. licensed financial institutions and other institutions which are subject to these Guidelines;
(b) Saint Lucian residents whose accounts/facilities are serviced solely either by salary deductions, or financing arrangements via regulated financial institutions.

Normal Risk Clients

The Company will accept Clients who are categorized as normal risk Clients as long as the general principles above are followed.

The following are the criteria set by the company to categorize a client as 'normal risk':

(a) any Client who does not fall under the 'low risk Clients' or 'high-risk Clients' categories.
(b) Clients who are not physically present for identification purposes (non-face -to-face Clients)

High Risk Clients

The Company will accept Clients who are categorized as high risk Clients as long as the general principles are followed.

Moreover, the Company will apply the Enhanced Client Identification and Due Diligence measures for high risk Clients.

High risk indicators:

(a) Intermediary arrangements (where the real or beneficial owner of the funds is not the facility holder); Anonymity factor;
(b) Financial service intermediaries that are not subject to prudential regulation;
(c) Non-Saint Lucian residents;
(d) Large cash transaction;
(e) Transactions from countries or jurisdictions which have inadequate AML systems. The following websites contain sources of relevant information for financial institutions—

(i) Office of Foreign Assets Control (OFAC) for information pertaining to USA foreign policy and national security: www.treas.gov.ofac,
(ii) Transparency International for information on countries vulnerable to corruption: www.transparency.org,
(iii) The Financial Crimes Enforcement Network (FINCEN) for country advisories: www.fincen.gov and;

(f) Persons resident in or maintaining trading operations in locations that are known to have significant established organized crime environments.
(g) Country Trends:
The following regions are considered to be high-risk in terms of laundering activities as per the Money Laundering Prevention Act:

- (i) Latin America,
- (ii) Pacific Rim Region,
- (iii) Central and South America,
- (iv) Central and Eastern Europe,
- (v) Africa (in particular, West Africa);

(g) Persons resident in or maintaining trading operations in known drug producing/transshipment locations;
(h) Persons from or maintaining trading operations in locations that are experiencing political instability or with a history of this;
(i) PEPs

The criteria for categorizing the clients using the risk based approach:

In this respect, the AMLCO shall be responsible to gather the said information and the said information shall be duly documented and filed, as applicable, according to the recording keeping procedures of this policy.

The said information shall be duly documented and filed, as applicable, according to the recording keeping procedures

Finally, the Company shall monitor on an ongoing basis the transactions of low risk Clients to ensure that there are no suspicious transactions.

The following is a non-exhaustive list of factors and types of potentially higher risk:

Client Risk factors:

(a) The business relationship is conducted in unusual circumstances;

(b) Clients that are resident in geographical areas of higher risk as set out in point e above;

(c) Legal persons or arrangements that are personal asset-holding vehicles;

(d) Companies that have nominee shareholders or shares in bearer form;

(e) Businesses that are cash-intensive;

(f) The ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(g) Politically Exposed persons

(h) Clients included in the leaked documents of Mossack Fonseca (Panama Papers)

(i) Clients convicted for a Prescribed Offense (and already served their sentence)

(j) Unwillingness of Client to provide information on the Beneficial Owners of a legal person.

(k) Trust accounts

(l) "Clients accounts" in the name of a third person

(m) Clients who are involved in electronic gambling/gaming activities through the internet

(n) Clients from countries which inadequately apply FATF's and CFATF (Caribbean Financial Task Force) recommendations or clients from jurisdiction listed by OFAC as well as any other relevant body the Company takes into consideration

(o) Any other Clients that their nature entail a higher risk of money laundering or terrorist financing

(p) Any other Client determined by the Company itself to be classified as such.

Product, service, transaction or delivery channel risk factors:

(a) Private banking;

(b) Products or transactions that might favor anonymity;

(c) Non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures or liveness checks or 2-factor authentication controls;;

(d) Payment received from unknown or non-associated third parties;

(e) New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

Geographical risk factors:

(a) Without prejudice countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

(b) Countries identified by credible sources as having significant levels of corruption or other criminal activity;

(c) Countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;

Risk based on the Client's behavior:

(a) Client transactions where there is no apparent legal financial/commercial rationale

(b) Situations where the origin of wealth and/or source of funds cannot be easily verified

(c) Unwillingness of Clients to provide information on the Beneficial Owners of a legal person.

Risk based on the Client's initial communication with the Company:

(a) Clients introduced by a third person.

Risk based on the Company's services and financial instruments:

(a) Services that allow payments to third persons/parties

(b) Services that request that facility of crypto-payments

(c) Large cash deposits or withdrawals

(d) Products or transactions which may favor anonymity.

Owing to the fact that the Company has determined that in certain cases there is low risk of AML/TF activities, and in order to ensure normal conduct of the business operations, the Company decided that:

a) in cases which are defined by the Company for the purposes of this policy as posing a lower risk of AML/TF, the Company decided to allow the client to use all of the Company's Investment and Ancillary Services for a limited period of time, after the completion of the Company's Registration Process but prior to the completion of the verification process (as this is described in AML Policy);

b) in cases which are defined by the Company for the purposes of this policy as posing medium risk of AML/TF, the Company the Company has decided to accept applicants only after the full verification of clients' identity;

c) in cases which are defined by this CAP as posing higher risk of ML/TF, the Company has decided to accept applicants only after the full verification of clients' identity;

Under no circumstance will the client be able to deposit with the Company's platform without first completing the registration and verification procedure (including Client due diligence (CDD) questionnaire and KYC (Know your Client procedure), thus providing sufficient details to complete the Identification procedure.

Under no circumstances will the client be able to utilize the full range of Investment and Ancillary Services without limitation via the Company's platform, prior to the full completion of the verification of client's identity by the Company (AML Approved).

The following list predetermines the type of Clients who are not acceptable for establishing a business relationship or an execution of an occasional transaction with the Company:

(a) 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;

(b) Shell Banks (the Company is prohibited from entering into, or continuing, a correspondent relationship with a shell bank. The Company will take appropriate measures to ensure that it does not engage in or continue correspondent relationships with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank);
(c) Clients included in Sanction Lists.
(d) Clients convicted for a Predicate Offense (and are yet to serve their sentence). Depending on the nature of Predicate Offense, it is at the Company's discretion not to accept a Client even after having served his/her sentence.
(e) Clients who are residents of certain jurisdictions including Iran,Russia and North Korea. The list of restricted jurisdictions will be based on FATF/CFATF and OFAC guidelines that might change from time to time, as well as the Company's own risk appetite.

In addition to the above, it shall be noted that the Company in order to ascertain the categories of clients who are not acceptable for establishing relationship or an execution of an occasional transaction, it shall takes into consideration factors such as the client's background, type and nature of its business activities, its country of origin, the services and the financial instruments applied for, the anticipated level and nature of business transactions as well as the expected source and origin of funds.

Taking into consideration the assessed risks, the Company will 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:

(a) adaption of the Client Due Diligence Procedures in respect of Clients in line with their assessed Money Laundering and Terrorist Financing risk
(b) 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)
(c) 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
(d) ongoing monitoring of high risk Clients' transactions and activities, as and when applicable.

Enhanced Due Diligence Measures and Procedures:

In cases of High Risk, or Medium Risk clients based on Company's internal Risk Classification Procedure and AML Policy (found during pre-trading process, or during post-trading), the Company will immediately start Enhanced Due Diligence (the "EDD") process, and apply EDD measures and procedures to the following Clients:

(a) Trust accounts
(b) Non-face-to-face Clients with no previous business relationship with Company and that were not introduced by existing clients: in case the Company identifies that the business relationship presents a higher risk of money laundering from illegal activities or financing of terrorism. The following measures should apply:
(i) The first payment of the operations is carried out through an account held in the Client's name with a credit institution operating and licensed in a third country, which has not been identified as high-risk third country, as well as in other cases of higher risk identified by the Company.
(ii) obtaining an original or true copy of a direct confirmation of the establishment of a business relationship of a business relationship through direct personal contact, as well as the true name, address, and passport/identity card number of the Client, from a credit institution or a financial institution, with which the Client cooperates, operating in Saint Lucia, United States, in any of the Member States or a third

country which has not been as high-risk third country, as well as in other cases of higher risk identified by the Company.
(iii) communication with the Client via post to an address, which the Company has already verified by independent and reliable sources.
(iv) contacting the Client via a telephone call at his home or office, on a telephone number verified by an independent and reliable source, during which the Company will confirm additional aspects of the identity information submitted by
(v) the Client during the Client account opening process. It is noted that the Company will keep records of the respective call.
(vi) requesting the client to undergo liveness verification checks
Additional Measures to mitigate risk may also include—

- Certification of documents presented
- Requisition of additional documents to complement those which are required for non-face-to-face customers, Independent verification of documents by contacting a third party.

(c) Accounts in the names of companies whose shares are in bearer form
(d) Clients from countries or geographical areas which do not apply or they apply inadequately FATF's or CFATF's recommendations on Money Laundering and Terrorist Financing:

(i) The Company exercises additional monitoring procedures and pays special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid recommendations.
(ii) Transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic, business or investment background and purpose. If the Company cannot be fully satisfied as to the legitimacy of a transaction, then a suspicious transaction report is filed to the Financial Intelligence Authority of Saint Lucia, according to the instructions given from the above said Unit.

(e) Where the Company is considering forming a business relationship with a person whom it suspects of being a PEP it will exercise enhanced due diligence to identify that person fully.

(f) if the Company maintains business relations with nationals and entities of countries that are vulnerable to corruption, then the relevant department will establish who the senior political figures in countries

which are vulnerable to corruption are and determine whether their customer has close links with such individuals (e.g. immediate family or close associates). The Company will also consider the risk that a customer may be susceptible to acquiring connections with such political figures after the business relationship has been established;

(i) exercising vigilance where their customers are involved in the type of business which appears to be most vulnerable to corruption, including trading or dealing in precious stones or precious metals.

The Company also will adopt detailed due diligence methods which should include—

(a) scrutinizing complex structures (those utilizing legal structures such as multiple corporate entities, trusts, foundations and multiple jurisdictions),
(b) establishing the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship, both at the onset of the relationship and on an ongoing basis
(c) developing a profile of usual and expected activity of the business in order to provide a basis for regular monitoring. The profile should be regularly reviewed and updated
(d) reviewing the decision to commence the business relationship at a senior management or at a Board level and reviewing the development of the relationship annually
(e) scrutinizing unusual features including very large transactions, the use of government or central bank accounts, expressed demands for secrecy, the use of cash, bearer bonds or other instruments which severs an audit an audit trail, the use of unknown financial institutions and repeated transactions involving sums just below a typical reporting level.

The information collected in accordance with the policies to be adopted by the Company will be fully documented and may constitute the basis upon which the financial institution avoids or terminates a business relationship with PEPs.

The Company will always adhere to the following key principles of monitoring PEPs as part of its enhanced due diligence procedures—

(a) ascertain identity of the account holder and the account's beneficial holder;
(b) obtain adequate documentation regarding the PEP;
(c) understand the PEP's anticipated account activity;
(d) determine the PEP's source of wealth;
(e) apply additional oversight to the PEP's account.

The Company will also take into consideration the following Money Lanudering prevention Act provisions as far as transaction sizes are concerned:

"Subject to sections 17(3)(b) and 17(4)(d) of the Money Laundering Prevention Act, a person who enters into a transaction with a financial institution or a person engaged in other business activity exceeding $25,000 shall fill out a source of funds declaration in the prescribed form.''

Transactions exceeding $25,000:

"A person who makes a false declaration in a source of funds declaration commits an offense and is liable on summary conviction to a fine not exceeding $50,000 or imprisonment for a term not exceeding 5 years. (Inserted by Act 20 of 2016)."

KYC Process Completion

When must Identity be Verified:

Whenever an account is to be opened, a new signatory added to an account, or a significant one-off transaction undertaken, the prospective customer must be identified. Once identification procedures have been satisfactorily completed, then the business relationship has been established and as long as records are maintained as required by the relevant AML Guidelines, no further evidence of identity is required when transactions are subsequently undertaken. However, irrespective of the exemptions noted in paragraphs 106 – 112 of the Money Laundering Prevention Act,identity must be verified in all cases where money laundering is known or suspected.

The Company will take reasonable measures to verify the true identity of a person seeking to enter into a transaction with or to carry out a transaction or series of transactions with the financial institution or person engaged in other business activity.

The Company will also establish and maintain identification procedures that require —

(a) an applicant to produce satisfactory evidence of his or her identity, in accordance with the guidance notes, as soon as practicable after first making contact with the financial institution or person engaged in other business activity;

(b) if satisfactory evidence is not obtained, that the business in question must not proceed any further shall only proceed in accordance with any direction, by the Authority.

The above provision applies to the following types of business —

(a) the forming of a business relationship;

(b) a one-off transaction where payment is to be made by or to the applicant of $10,000 or more;

(c) two or more one-off transactions that —

(i) appear to a person handling the transaction on behalf of the regulated institution to be linked, and

(ii) in respect of which, the total amount payable by or to the applicant is $10,000 or more;

(d) where in respect of a one-off transaction a person handling the transaction on behalf of the financial institution or person engaged in other business activity knows or suspects —

(i) that the applicant is engaged in money laundering, regardless of the amount of the transaction

(ii) that the transaction is carried out on behalf of another person engaged in money laundering.

The Compliance Department will approve, or not approve the client whilst taking into account all the overall aspects raised from the due diligence procedure.

For Client Monitoring Purposes, the Compliance Department will classify the client's risk according to the various parameters detailed in the Company's internal Risk Classification Procedure.

In addition, the KYC documents of the clients will be monitored on an on-going basis to identify if at any time during the business relationship, adequate data and information are missing from the clients' file or need to be updated. The Company will take all the necessary actions, by applying the customer identification and due diligence procedures according to the Regulation.

Identification procedures and Client due diligence requirements will be applied not only to all new Clients but also to existing Clients at appropriate times depending on the level of risk of being involved in money laundering or terrorist financing.

Client Identification Procedure

Electronic Verification Process

During the Registration process, the Company will first perform the electronic verification of the client. As such, the Company is using 3rd party verification system which must fulfill the below conditions:

(a) Is registered with the Data Protection Commissioner in the country from which it operates, for the purposes of safety or the personal data and
(b) Electronic databases provide access to information that refers to both current and previous situations that indicate that the person actually exists and include positive information (at least full name, address and date of birth of the Client) as well as negative information (eg committing offenses such as identity theft, inclusion in files of deceased persons, inclusion in lists of sanctions and restrictive measures by the Council of the European Union and the Security Council UN).
(c) Uses multiple sources of information which update in real-time as well as present alerts whenever information in the system regarding a verified client, will change (eg. A previously verified client has now been added to a sanctions list)
(d) Provide details as to what kind of information was researched and resulted in either validation or invalidation of the client's verification
(e) Allows the Company to keep records of the information that was verified as well as the verification results
(f) electronic databases contain a wide range of sources, with information from various time intervals, updated to real-time update and send notifications trigger alerts when important data is differentiated
(g) has established transparent procedures that allow the Company to identify what information has been searched for, which ones are their effects and their importance in relation to the degree of certainty as to the identity of the Client.

In addition to the above the identification information, indicatively should come from two (2) or more sources. As a minimum, the electronic verification should match the following pattern:

(a) Match of the Full Name of the clients as well as his/her current Address of the client from one source, and
(b) Match of the Full Name of the client and his/her current address or date of birth, from a second source
(c) for purposes of performing identity authentication by electronic means, the Company must establish procedures to ensure the integrity, validity and reliability of the information it has access to, provided that the audit process should include both positive and negative information.

The Company establishes mechanisms for execution quality controls to evaluate the quality of information in which it intends to build.

The electronic verification takes place as soon as the client completes the Account opening questionnaire.These details are verified in the electronic verification system manually by the Account Opening operators who verify the clients one by one, ensuring this way a very high verification rate of clients from the very first steps of the registration.

The electronic verification is the primary mode of verification employed by the Company, however verification on the basis of documents can also be performed in conjunction with electronic verification or as an alternative, on a case by case basis and where deemed necessary:

a) A client resides in a country not covered by the electronic verification database
b) A client's details (eg. address) cannot be fully verified by minimum of two sources used by the electronic verification software
c) For performing account monitoring
d) Economic profile has made it necessary due to significant increase in monetary transactions
e) For AML investigation purposes
f) For Complaints investigation purposes

Individual Accounts

To Verify Client's account, Clients are required to upload both a proof of identity (POI) and proof of address (POA). Only after they provide us with both documents will the verification process begin.

The relevance and usefulness in this context of the following information should be considered—

(a) full name/s used;
(b) date and place of birth;
(c) nationality;
(d) current permanent address including postal code (Any address

printed on a personal account cheque tendered to open the account, if provided, should be compared with the address);
(e) telephone number;
(f) occupation and name of employer (if self employed, the nature of the self employment); and
(g) specimen signature of the verification subject (if a personal account cheque is tendered to open the account, the signature on the cheque should be compared with the specimen signature).

Proof of Identity:

As proof of identity:

- Passport
- Identity Card
- Driving License
- Armed forces identity card

The POI document should be valid, contain the Client's name, date of birth, a clear photograph, issue date and if it has an expiry date, that should be visible as well. The document should be photographed or scanned at a good resolution without cut edges and in focus and in color.

If the document is a passport then both pages of the passport should be clearly visible.If the document is double-sided, then both sides should be uploaded as well.

Proof of address:

The proof of address document should contain the Client's full name, residential address (not PO BOX) and an issue date which should not be older than 3 months. The name of the logo of the issuer should also be clearly visible. Client needs to make sure that he has photographed or scanned his document against a different-colored background, so that all four corners are visible.

The proof of address can be one of the following:

- Bank document (bank statement, credit card statement or bank letter)
- Utility Bill (electricity, water, gas), landline bill or internet bill connected to a landline
- Council tax bill
- Letter from your local municipality

The Company does not accept screenshots or digitally modified documents.

In the event that a Client submits a third country POI and an EU POA our Compliance

Team will request a residence permit card or a local Unique Identification Number proof.

Liveness Check:

Client stands in front of his camera and selfies are produced along with a very short video.

Corporate Accounts

- Certificate of Incorporation and certificate of good standing (where available) of the legal person
- Memorandum and articles of association.
- Certificate of Good Standing or equivalent.
- Certificate of Shareholders.
- Certificate of Directors and Secretary
- Certificate of Registered Office or equivalent.
- A resolution of the Board of Directors to open an account and confer authority to those who will operate it.
- In the cases where the registered shareholders act as nominees of the beneficial owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the beneficial owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the beneficial owner has been agreed.
- documents and data for the verification, the identity of the persons that are authorized by the legal person to operate the account, as well as the registered shareholders and beneficial owners of the legal person.
- Copies of the latest audited financial statements (if available).
- All accounts signatories should be duly accredited by the Company.

The relevance and usefulness in this context of the following documents(or their foreign equivalent) should also be carefully considered—

(a) The most recent annual return filed with the Registrar, duly notarized where such corporate body is incorporated outside Saint Lucia if applicable;

(b)The name(s) and address(es) of the beneficial owner/s or the person/ s on whose instructions the signatories to the account are empowered to act;

(c) Resolution, Bank Mandate, signed application form or any valid account opening authority, including full names of all directors and their specimen signatures and signed by no fewer than the number of directors required to make up a quorum;

(d) Copies of identification documents and authorized signatures should be

obtained from all directors in accordance with the general procedure for the verification of the identity of individuals;

(e) copies of Powers of Attorney or other authorities given by the directors in relation to the company if applicable;

(f) a signed director's statement as to the nature of the company's business if deemed necessary;

(g) a statement of the source of funds and purpose of the account should be completed and signed. This should show the expected turnover or volume of activity in the account;

(h) for large corporate accounts, the following may be obtained:

(i) annual reports/audited financial statements

(ii) description and place of principal line(s) of business, list of major business units, suppliers and customers, etc. where appropriate; a

As legal controls vary between jurisdictions, particular attention may need to be given to the place of origin of such documentation and the background against which it is produced.

Intermediaries

If the intermediary is a locally regulated institution and the account is in the name of the institution but on behalf of an underlying customer (perhaps with reference to a customer name or account number), this may be treated as an exempt case but otherwise the customer himself (or other person on whose wishes the intermediary is prepared to act) should be treated as a verification subject.

Updating of Documentation

Once Client has opened a live trading account with Virtual Markets, the Company is obligated to keep all clients' documentation up to date, therefore Client will be required to replace any expired document with an updated one when necessary.

Additionally, throughout the business relationship with the Company and in line with the Anti-Money Laundering regulations, verification will take place depending on the frequency or amount of certain transactions. This verification consists of information in regards to the Client's source of funds, where he will be required to state and prove his source of funds accordingly.

The company reserves the right to request any other documentation if appropriate to maintain adequate records for Client's profile validation.

Failure to provide the requested documentation may result in either closing the account or may not be able to provide the services required.

Deposits and Withdrawals

Deposits

(a) The Company will request/obtain documentation/information (i.e. bank statement or SWIFT confirmation) showing the bank account, the name of the Client and the amount that was sent to Company designated bank account for Clients' funds, in order to verify the depositor's details and identify the source of funds

(b) The Company reserves the right to reject the incoming transaction(s) in case where the bank account from where the funds were sent is not matching the Client's bank account as seen either on the statement, SWIFT or other similar reliable document/on-line banking interface, and return the funds to the remitter by the same method as they were received

(c) Deposits via Credit Card are automated for the Clients who have enabled the 3D Secure option in their credit card settings. For those who are identified by the Payment Provider that they do not have 3D Secure, then a copy of their credit card may be requested showing the first and the last 4 digits of the card, the name and expiry date of the card.

(d) The Company reserves the right to request from the Client additional documents/information (e.g. bank/card statement showing inter alia depositor's name, account number and transaction done to the Company) in case where the copies of the card provided do not bear the necessary information.If the Company is still not satisfied as to the above (i.e. could not identify the source of funds) then we will reject the incoming transaction(s) and return the funds to the remitter by the same method as they were received.

Withdrawals

Upon receiving an instruction from the Client through their client area to withdraw funds from their account, the Company will process the withdrawal request on the same day that the request was made, or the next working day if the client's request is received outside of normal business trading hours, only if the following requirements are met:

a) the withdrawal instruction includes all necessary information in the client area;

b) the instruction is to make a transfer to the originating account (whether that is a bank account, a payment system account etc.) from which the money was originally deposited in the Account or at the Client's request to a bank account belonging to the Client.

*In case of credit/debit card deposits, where the refundable amount exceeds the deposited amount (i.e. Client made profits), then the exceeding amount will be sent

by bank wire or another payment method, unless there is credit card assuring through supporting documents (i.e. account statement) that the bank account or funding method account to which the profits will be sent belongs to the Client.

c) the account where the transfer is to be made belongs to the Client.

d) at the moment of payment, the client's balance exceeds the amount specified in the withdrawal instruction including all payment charges;

e) there is no Force Majeure event which prohibiting the Company from effecting the withdrawal and

f) the Client must be fully verified according to Verification guidelines set forth in this Policy and the Client Agreement.

Third party or anonymous payments

(a) The Company reserves the right not to comply with any request by the Client to make a payment or a delivery to a third party or in case of anonymous accounts.

(b) If the Company becomes aware that funds have been paid or delivered to Virtual Markets by a third party, or in case of anonymous transactions, Virtual Markets reserves the right to refuse such payment or delivery and such payments will not be added in the Client's Trading Account or E-Wallet Account.

(c) In case the Company becomes aware that funds have been paid or delivered to the Company by a third party or in case of anonymous transactions, the transferred funds will be refunded back to the same payment details from where they have been paid. The Client will be charged with all costs for the refund transaction.

Training Obligation

The Company ensures that its employees, its contractors and others participating in the business on a similar basis and who perform work tasks that are of importance for preventing the use of the business for money laundering or terrorist financing ('Relevant Persons') have the relevant qualifications for these work tasks.

When a relevant person is recruited or engaged, the Relevant Person's qualifications are checked as part of the recruitment/appointment process by carrying out background checks comprising extracts from criminal records in addition to the customary taking of references, which is documented using a special standard form assessing employee suitability.

In accordance with the requirements applicable to the Company on ensuring the

suitability of relevant persons, the Company makes sure that such persons receive appropriate training and information on an ongoing basis to be able to fulfill the Company's obligations in compliance with the applicable legislation. It is ensured through training that such persons are knowledgeable within the area of AML/CFT to an appropriate extent considering the person's tasks and function.

The training must provide, first and foremost, information on all the most contemporary money laundering and terrorist financing methods and risks arising therefrom.This training refers to relevant parts of the content of the applicable rules and regulations, theCompany's risk assessment, the Company's AML Policy and procedures and information that should facilitate such Relevant Persons detecting suspected money laundering and terrorist financing. The training is structured on the basis of the risks identified through the risk assessment policy.

The content and frequency of the training is adapted to the person's tasks and function on issues relating to AML/CFT measures. If the Policy is updated or amended in some way, the content and frequency of the training is adjusted appropriately.

For new employees, the training comprises a review of the content of the applicable rules and regulations, the Company's risk assessment policy, these Guidelines and other relevant procedures.

The employees and the Management Board members receive training on an ongoing basis under the auspices of the AMLRO in accordance with the following training plan: periodicity: at least once a year for the Management Board members.

At least once a year for the Company's employees and relevant person engaged. scope: review of applicable rules and regulations, the Company's Guidelines and other relevant procedures. Specific information relating to new/updated features in the applicable rules and regulations. Report and exchange of experience relating to transactions reviewed since the previous training.

In addition to the above, relevant persons are kept informed on an ongoing basis about new trends, patterns and methods and are provided with other information relevant to the prevention of money laundering and terrorist financing.

The training held is to be documented electronically and confirmed with the relevant person signature. This documentation should include the content of the training, names of participants and date of the training.

The Company will record. tt a minimum, records should be maintained on the following—

(a) details and contents of the training programme;

(b) names of staff receiving training;
(c) dates of training sessions; and
(d) assessment of training.

Institutions have a duty to ensure that key staff receive sufficient training to alert them to the circumstances whereby they should report customers/clients or their transactions to the Compliance Officer. Such training should include making key staff aware of the basic elements of—

(i) the Act and any Regulations made thereunder, and in particular the personal obligations of key staff thereunder, as distinct from the obligations of their employers thereunder;
(ii) vigilance policy and vigilance systems;
(iii) the recognition and handling of suspicious transactions;
(iv) other pieces of anti-money laundering legislation identified at the beginning of this Policy;;
any Code of Conduct/Practice issued under regulatory legislation or voluntarily adopted by various industry associations; and any additional guidelines and instructions issued by the FIA.

The effectiveness of a vigilance system is directly related to the level of awareness engendered in key staff, both as to the background of international crime against which the Act and other anti-money laundering legislation have been enacted as well as to the personal legal liability of each of them for failure to perform the duty of vigilance and to report suspicions appropriately.

Training Programmes

While the Company should decide for itself how to meet the need to train members of its key staff in accordance with its particular commercial requirements, the following programmes will usually be appropriate—

General induction training should include:

(a) the company's instruction manual;
(b) a description of the nature and processes of laundering;
(c) an explanation of the underlying legal obligations contained in the Act and any Regulations made thereunder; and other anti-money laundering legislation and guidelines;
(d) an explanation of vigilance policy and systems, including particular emphasis on verification and the recognition of suspicious transactions and the need to report suspicions to the Compliance Officer (or equivalent).

Collection and Preservation of data

The Company through the person (incl. Employees, Management Board members and AMLRO) who firstly receives the relevant information or documents shall register and retain:

- all data collected within CDD measures implementation;
- information about the circumstances of refusal of the establishment of the business relationship by the Company;
- the circumstances of the refusal to establish business relationship on the initiative of the customer
- if the customer refusal is related to the application of CDD measures by the Company;
- information on all of the operations made to identify the person participating in the transaction or the Customer;
- beneficial owner;
- information if it is impossible to take the CDD measures using information technology means; information on the circumstances of termination of the business relationship in connection with the impossibility of application of the CDD measures the each transaction date or period and a description of the contents of the transaction;
- information serving as the basis for the reporting obligations specified above; data of suspicious or unusual transactions or circumstances of which the FIA was not notified.

In addition to the above mentioned information the Company willl register the following data:

(a) regarding a transaction upon opening an account:
- the account type, number,
- currency and significant characteristics of the securities or other property;

(b) upon making a payment relating to shares, bonds or other securities:
- the type of the securities
- the monetary value of the transaction
- the currency and the account number

(c) in the case of another transaction:

- the transaction amount
- the currency
- account number.

Other relevant responsibilities of the Company:

(a) to establish and maintain transaction records for both domestic and international transactions for a period of seven years after the completion of the transaction recorded;
(b) establish and maintain a record that indicates the nature of the evidence obtained and which comprises either a copy of the evidence or information as would enable a copy of it to be maintained;
(c) report to the Authority a transaction where the identity of a person involved in the transaction or the circumstances relating to the transaction

Records with regard to activity suspicions:

(a) Record of any suspicion report of any employe to AMLRO
(b) Record THE report to the Authority
(c) Notes of any actions taken
(d) Record outcomes of inspections
(e) record requests by any relevant authority in Saint lucia or other jurisdictions

The Company will keep a record —

(a) if the record relates to the opening of an account with the financial institution for a period of 7 years after the day on which the account is closed;
(b) if the record relates to the renting by a person of a deposit box held by the financial institution, for a period of 7 years after the day on which the deposit box ceases to be used by the person; or
(c) in any other case, for a period of 7 years after the day on which the transaction recorded takes place.

Documents and data must be retained in a manner that allows for exhaustive and immediate response to the queries made by the FIA or, pursuant to legislation, other supervisory authorities, investigation authorities or the court.

The Company implements all rules of protection of personal data upon application of the requirements arising from the applicable legislation. The Company is allowed to process personal data gathered upon CDD implementation only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

The Company deletes the retained data after the expiry of the time period, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a precept of the competent supervisory authority, data of importance for prevention, detection or investigation of money laundering or terrorist financing may be retained for a longer period, but not for more than five years after the expiry of the first time period.

Avoiding Conflict of Interests

The Employees (incl. AMLRO) must avoid the conflict of interests and when this happens,immediately notify the Management Board member or the AMLRO.

The conflict of interests is understood as all the circumstances known to the Company or its employees that may affect the decisions of making a transaction or establishing business relationship and which do not correspond to the interests of the Company or its customer.

To achieve the goal of avoiding the conflict of interests, the Company shall collect and regularly update its employee's data in order to identify their interests in the context of preventing money laundering and terrorist financing.

The Company collects the following data about each employee: the birthplace and place of residence of the employee; other job positions and contracts of the employee that they have in the context of the economic field;the data regarding the close relatives of the employee (spouse, parents, children, siblings and their children): for each person, their place of residence and place of work. other data known to the employee which may indicate the interests in the context of preventing money laundering and terrorist financing.

The failure of the employee to provide the data specified above is considered to be a significant violation of the employment contract and may result in the extraordinary cancellation of the employment contract for reasons arising from the employee.

The Company identifies and analyses, inter alia, whether the persons directing customers to the Company (e.g. agents, resellers, etc.) have any interests regarding the Customer (e.g., provide them with legal services, accounting services, services providing the establishment of companies and other legal structures, etc.) which cause the conflict of interests between the person directing customers to the Company and the Customer.

In case of identifying a conflict of interests or circumstances indicating a conflict of interests, the Company shall apply all necessary measures to prevent it. If it is impossible to prevent the conflict of interests, the Company must not conclude any transactions or establish the business relationship. The Management Board is responsible for avoiding conflict of interests in the Company.