Policy for preventing Money Laundering and Terrorism Financing SimpleFX Ltd.

Approval Date:

. 12/03/2018

Type of approval/update

Approved upon the Resolution of Board of Directors

Summary:

SimpleFX Ltd. (“the Company”) aims to prevent, detect and not knowingly facilitate money laundering and terrorism financing activities. The Company does this to protect its reputation, to comply with relevant laws and requirements, as well as to be a good corporate citizen. The Company also aims to comply with anti-money laundering (“AML”) and counter-terrorism financing (“CTF”) recommendations in a way that complements business priorities.

The management of the Company places extremely high importance on assisting in discovering any money laundering scheme. These policies are to be read by and adhered to by all employees and officers of the Company. Any employee found not to be adhering to these policies and procedures will face severe disciplinary action.

It is the policy of the Company and its Collaborators to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities.

The due to entirely cross - boarder character of the performing transactions, covered hereby, the international legal framework for anti - money laundering consists of a number of sources represented by international conventions, the FATF Recommendations, European as well domestic law provisions.

The following table indicates the main reference rules for the Company, in relation to the countries in which it operates under the right of establishment. It should also be noted that for the purpose of the Company’s activities operations in the counterparts’ jurisdictions.

Source of legislation Legislative Description reference
FAFT Recommendations: Recommendations of FATF - FATF IX Special Recommendations, FATF 40 Recommendations. They represent the fundamental standards on preventing and combating money laundering and terrorism financing, to which other international bodies, the European Union and individual Member State refer.
Community - EU EU Directive – 2015/849 – IV Anti - money laundering It sets out measures for preventing and combating money laundering and terrorism financing, acknowledging, over time, the evolution of international standards with the aim of achieving a harmonised regulatory environment between the Member States.
Domestic law of St. Vincent and the Grenadines' The Proceeds of Crime Act, No. 38 of 2015; The Financial intelligence Unit Act, Cap 174 of the Revised Laws of 2009, as amended by Act No. 7 of 2013; The Drug Trafficking Offenses Act, Cap 173 of the Revised laws of 2009; The Exchange of Information Act, cap 146 of the Revised Laws of 2009; The Proceeds of Crime and Money Laundering (Prevention) Act, 2001 The Proceeds of Crime and Money Laundering Regulations, 2002 The Financial Intelligence Unit Act, 2001 The Mutual Assistance in Criminal Matters Act, cap 177 of the Revised Laws of 2009; The Anti- Money laundering and Terrorist Financing Regulations, No. 20 of 2014;

The Confiscation in the Magistrates' Court Regulations, No. 22 of 2015.

St. Vincent and the Grenadines has implemented a package of legislation aimed at detecting, preventing, and prosecuting money laundering and other serious crimes as well as confiscating the profits of crime. The legislative measures reflect international best practices and take account of the 40 Recommendations of the Financial Action Task Force (FATF) on money laundering and the 19 Recommendations of the Caribbean FATF.

The regulatory body with the mandate to supervise the offshore financial sector is the Financial Services Authority.

The above-mentioned provisions are likely to be amended / integrated / replaced following the full transposition - in the jurisdictions in which the Company operates – of EU Directive - 2015/849 - "*IV Anti - Money Laundering Directive*".

2. Definitions:

1. **"Anti - Money Laundering (AML) Officer or Anti-Money Laundering (AML) Function of the Company"** shall mean the Compliance and AML Officer of Company.
2. "**Company"** shall mean SimpleFX Ltd. with its registered office in Kingstown, at Suite 305th (Griffith Corporate Centre), Saint Vincent and Grenadines under IBC Number 22361.
3. "**Board of Directors"** shall mean the "*management body*" of the Company, i.e. to which ordinary management duties, namely the management of the all Company's affairs related to any scope of its commercial activities and representation of Company beyond third parties, court and any authorities in line with the rules and representation of the Company.
4. "**Policy"** shall mean this Policy for preventing Money Laundering and Terrorism Financing SimpleFX.
5. "**Collaborators"** shall mean each Legal Entity or Natural Person in, both domestic and foreign, regardless of legal form (e.g. companies, partnerships, investment funds, mutual funds etc.), which is known to have close business relations related to the common commercial activities, provided by leadership of Company, including outsourcing or insourcing of the particular fraction of business activity of the Company (e.g. IT; Customer's help desk; marketing services; customer service).
6. **"Natural Person"** shall mean a person (in legal meaning, i.e., one who has its own legal personality) that is an individual human being, as opposed to a legal entity, which may be a private (i.e. business entity or non-governmental organisation) or public (i.e. government) organisation.
7. **"Legal Entity"** shall mean any form of legal persons, both domestic and foreign, regardless of legal form, such as without limitation corporate entities, trusts, foundations, and legal arrangements similar to trusts, (e.g. companies, partnerships, investment funds, mutual funds etc.).
8. "**Transaction"** shall mean any deposit, withdrawal, exchange or transfer of funds.
9. "**Crypto currency"** shall mean a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. Cryptocurrencies are classified as a subset of digital currencies and are also classified as a subset of alternative currencies and virtual currencies. For the purposes of the Company's business activity crypto currency is treated as the commodity. It is emphasised that exchanging the crypto currencies for fiat currency within Company business model is strictly prohibited.
10. **"Fiduciary/ Fiat Currency"** shall mean a currency without intrinsic value established as money by government regulation. It has an

assigned value only because the government uses its power to enforce the value of a fiat currency.

11. "**Customer**" shall mean Natural Person(s) and Legal Entity(Entities) who has opened CFD Account in SimpleFX Ltd. with respect of fiat currency and crypto currency.
12. **"CFD"** shall mean a contract for differences as a contract between two parties, typically described as "buyer" and "seller", stipulating that the seller will pay to the buyer the difference between the current value of an asset and its value at contract time (if the difference is negative, then the buyer pays instead to the seller). In effect CFDs are financial derivatives that allow traders to take advantage of prices moving up (long positions) or prices moving down (short positions) on underlying financial instruments.
13. "**CFD account**" shall mean trading account and fund account collectively.
14. "**Prominent Public Functions"** shall mean persons, who have been entrusted with prominent public functions are:
    - heads of State, heads of government, ministers and deputy or assistant ministers;
    - members of parliament or of similar legislative bodies;
    - members of the governing bodies of political parties;
    - members of supreme courts, of constitutional courts or of other high - level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
    - members of courts of auditors or of the boards of central banks;
    - ambassadors, chargés d'affaires and high - ranking officers in the armed forces;
    - members of the administrative, management or supervisory bodies of State - owned enterprises;
    - directors, deputy directors and members of the board or equivalent function of an international organisation.
15. "**Close Family Members"** shall include the following:

    a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

    b) the children and their spouses, those who in the last five years have lived with or persons considered to be equivalent to a spouse, of a politically exposed person

16. "**Persons known to be Close Associates**" shall mean:

    a) Natural Persons who are known to have joint beneficial ownership of Legal Entities or legal arrangements, or any other close business relations, with a politically exposed person;

b) Natural Persons who have sole beneficial ownership of a Legal Entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

3. Anti - money laundering and terrorism financing Policy of the SimpleFX

The SimpleFX (hereinafter referred to as: the "**Company**") is aware of the importance of countering the phenomena of transferring, concealing and covering up of proceeds from illegal activities.

To this end, operational activities undertaken by the Company are carried out in full compliance with applicable anti - money laundering legislation and regulations issued by the competent authorities, each part of the country in which the Company operates, refusing to engage in suspicious transactions in terms of fairness, transparency, ethical business and starting relationships with financial and trade counter-parties, suppliers, partners, contractors and consultants, only after checks on the information available relating to their respectability and the legitimacy of their activity, so as to avoid any implication in operations able, even potentially, to favour the laundering of money from illegal or criminal activities, and acting in full compliance with internal Compliances and AML procedures and anti - money laundering legislation. Based on these principles, the present Anti - Money Laundering and Anti - terrorism financing Policy of the SimpleFX Ltd. (hereinafter referred to as: the "**Policy**") transposes the obligations in this regard, with particular reference to:

a) general principles of the risk management model for money laundering and terrorism financing and related strategic guidelines for the Company;

b) responsibilities and duties of the social and business structures;

c) operating procedures for risk management of money laundering and terrorism financing, where it is recommended to improve the management process in this scope.

In particular, it aims at:

- empowering all the personnel of the Company;
- clearly defining, at various organisational levels, roles, tasks and responsibilities in this regard;
- describing an architecture of internal Compliance and AML functions to be coordinated into its components, including through appropriate information flows, which is to be also in line with the articulation of the structure, the complexity, the dimension of the Company, the types of transactions offered as well as the amount of risk associated with the characteristics of Customers with whom the Company operates;
- setting out adequate flows of information on the monitoring activities carried out in the field.
- The Policy has been approved by the Board of Directors of the Company and implemented by all Collaborators, and is constantly

updated by the Compliance and AML Officer of the Company and made available to all members of the staff in particular, the Compliance and AML Officer - in the event of non - formal amendments to the Policy - in addition to training courses in any case already planned for the period, provides for an “ad hoc” updating training session.

3. Definition of money laundering and terrorism financing

1) MONEY LAUNDERING

Money laundering is one of the most serious criminal activities in the financial market. The reinvestment of criminal proceeds in legal activities profoundly disturbs the market mechanisms, affects the efficiency and fairness of the financial activity and weakens the economic system itself. The risk of money laundering or terrorism financing in financial institutions is manifested in the form of involvement, even inadvertently, in these phenomena. (for example, tax evasion, false accounting, robberies), the redeployment of the proceeds from illegal funds in order to make invisible the offence that gave rise to these funds and reinvestment thereof in lawful economic activities the proceeds in order to shrink the huge volumes of cash generated by criminal activity. These proceeds include those derived from a variety of criminal activities including tax evasion, terrorism, sale of drugs, corruption, theft, etc. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Pursuant to the Legal Framework of European Union, the money laundering shall be regarded as the following conduct, when committed intentionally:

a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;

b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

2) THE FINANCING OF TERRORISM

The financing of terrorism is defined as any activity aimed at, by any means, the supply, collection, brokerage, deposit, custody and disbursement of funds or economic resources, in any way made, intended to be, in whole or in part, used in order to commit one or more crimes related to terrorism or in any case designed to encourage the commitment of one or more crimes for purposes of terrorism under the criminal code, regardless of the actual use of funds and economic resources for the commission of the aforementioned crimes.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Thus, while for the offence of money laundering the origin of values or property is of fundamental importance (which must be of an illegal origin), for the financing of terrorism it is necessary to assess their purpose, which is to perform or to facilitate the commitment of one or more crimes with terrorist intent.

Therefore, the preventive measures covered by this Policy are intended not only to counter the use of the values derived from crime but also to prevent the implementation of any activities that could be tracked down to terrorism financing activities.

4. Obligations and prohibitions

The Company, pursuant to the binding laws and regulations, as well incorporated FAFT Recommendations and EU Directives observes specific obligations - on subject and in compliance with the specific rules applicable in the individual jurisdictions - relating to:

- identification and Customer due diligence (so called "***Know Your Customer***");
- establishment, registration and storage of data collected in a special archive designed and managed by means of IT systems, in relation to activities carried out in by the Company;
- reporting of Anti - Money Laundering Notifications, where it's applicable and notifications of suspicious transactions upon the Suspicious Transactions Reports ("STR") to the respective supervisory authorities;
- adoption of measures aimed at ensuring confidentiality of the identity subjects that trigger the enhanced verification process and/or make the notification;
- continuous training and information activities for all the staff guaranteed by the Company.

In particular, the identification and adequate verification of Customer data and the possible executing entity is made on the basis of documents, data or information provided by them or coming from a reliable and independent source. The Company refrains from establishing/continue a business relationship or carrying out a transaction operation in the case it is not able to fulfil the obligations of identification and Customer Due Diligence.

The due diligence is modulated, in terms of intensity and extension, based on the risk of money laundering and terrorism financing, following a "*risk - based approach*", which aims at maximising the effectiveness of business controls, rationalising the use of resources and reducing the burden of the recipients.

The obligations for registration and retention of data are aimed at making it possible to search and use of such data in the investigation on cases of money laundering or terrorism financing and for the analysis by the respective supervisory authorities. The registration of data in the electronic archive for anti - money laundering is made promptly and in any event within the time limits established by the existing regulations.

In order to ensure the proper fulfilment of obligations to combat money laundering and terrorism financing, the Company:

- adopts suitable **processes, tools and controls** that allow for full respect of the principles contained in this Policy;
- ensures adequate, complete and timely **information flows** to and from the corporate bodies, top management, control and operational structures;

- provides **training** and educational programs aimed at the constant updating of the personnel;
- enforces internal organisational safeguards for the prevention of predicate crimes of administrative liability of the Company. In this context, the prohibitions and cautions provided by the Company Code of Ethics shall be integrally considered, with regard to relations with bodies in relation to which there is reasonable suspicion that they are involved in illegal activities;
- adopts an approach of shared risk between the different types of transactions.

In particular, the Company shall:

a) refrain from establishing relationships with individuals for whom the due diligence process has not been completed, reasonably promptly in terms of fiat currency and within 30 days with respect of existing crypto currencies accounts. Any exceptions must be submitted to the authorisation of the Board of Directors, granted upon its the relevant resolution;

b) give full effect to the legislative provisions foreseen in relation to the identification of the beneficial owner; in particular, in relation to companies, the beneficial owner is identified with the Natural Person or Natural Persons who ultimately own or control the Legal Entity. This requirement is satisfied where whenever it is possible to identify the individual person in position of Managerial Body <senior managing official(s)> and as well an individual person or some people who holds a percentage in the share of the capital of higher than the 25 percent plus one or an ownership interest of more than 25 percent;

c) take all necessary steps to determine and verify the true identity of the Customer and of any beneficial owners;

d) acquire, in the case of Customers with company shares held through trust companies, or in the case of foundations, trusts or non - profit organisations, a specific certification regarding the identity of the beneficial owner. It is also prohibited to open so called "Omnibus" accounts payable to trust companies and/or financial intermediaries. Any exceptions must be submitted to the authorisation of the Board of Directors, granted upon its the relevant resolution;

e) provides for specific internal authorisation processes depending on the risk profile of Customers: the establishment of ongoing relationships between entities of "high" risk profile is subject to the authorisation of the Board of Directors upon the relevant resolution;

f) apply enhanced due diligence measures in cases where:

- the transactions operations or the ongoing relationships involve politically exposed persons (PEPs) and persons living in the country who are or have been entrusted with Prominent Public Functions (PPF);
- **Politically exposed persons (PEPs)** are physical persons who are resident in the countries, who are or have ceased from less than an year to having been entrusted with prominent public functions, as well as their Close Family Members or those with whom such persons are **known to be Close Associates**. It's understood that, if the relevant local laws and regulations may provide a different definitions, in that case the Company will comply with their specific relevant laws and regulations.
- a high risk of money laundering emerges on the basis of objective and documented evidence (for example: the presence of a beneficial owner with the residence in an "not cooperating" country);
- the transaction, operations or the continuous relationships are reported to subjects with citizenship in countries considered "not cooperating";
- a notification on suspicious transaction has been sent to the relevant Supervisory Authority, in which case the Company applies reinforced measures as long as it considers that it can rule out the existence of a high risk of money laundering;
- a notification of a suspicious transaction has been sent to respective Supervisory Authority, in which case the Company applies reinforced measures as long as it considers that it can rule out the existence of a high risk of money laundering;

g) there is intervention by the Company's operating structures about any suspicion about a Customer's entity name (such as the possible presence of the name on anti - money laundering/anti - terrorist lists); it constantly checks that its Customers are not included in national or international blacklist;

h) refuse to carry out transactions involving in any way subjects entered in national or international blacklists, sanction lists, embargo lists (UN, OFAC, Communitarian);

i) not have relations, relationships, operation transactions with banking companies that have no physical presence in the country in which they are established and authorised to carry out their activities (SO - CALLED "*shell banks*");

j) restrict the use of cold hard cash as part of operation transactions carried out;

k) ensure sharing in respect of any confidentiality constraints imposed by local legislation in force, the names of the subjects reported to the respective national supervisory authorities for suspicious transactions.

5. Company's risk management model regarding money laundering and financing of terrorism

Proper management of risk of money laundering and terrorism financing is also ensured by the following principles:

- identification and appointment of an Anti - Money Laundering Officer;
- periodic exchange of information flows between the functions for the Anti - Money Laundering of the Company and the relevant personnel, involved in Know Your Customer process;
- transposition of this Policy by all Collaborators, so that they are fully aware of the risk of money laundering and terrorism financing management model established in accordance with their national regulations of reference and with best practices in the field.

For the prevention of the phenomena of transfer, concealment and cover - up of the proceeds from illegal activities, each Collaborator has adopted its own model / local regulation / procedure /guidelines for the management of compliance steps in this regard, inspired by this Policy, indicating the principles contained therein and the regulatory provisions locally applicable.

Each Collaborator, appoints a local Anti - Money Laundering Officer is , who reports to the Management Board or the similar managerial corporate body, as well General Partner(s) of the Collaborators. For the purpose of determining the risk of money laundering and terrorism financing, the Company has a policy that provides for the identification of criteria. In particular, the a structured process has been defined, which provides for:

- an initial assessment by the operational functions on clients' names, reported on anti - money laundering/anti - terrorism lists from adopted relevant on - line data;
- an enhanced Customer due diligence carried out by the relevant personnel, in the case of existence of doubts and/or incomplete information on the documents provided by a Customer, which may prejudice, partly as a result of the carried out investigations, the association between the client and the subject of the transaction;
- a possibility of adopting the automatic attribution by the computer system used, potentially, after the activities listed above, of the Customer money - laundering risk profile, based on criteria and conditions between the transaction based on fiat currency or crypto currency, in relation to different types of transactions provides from the latter.

5.1. Roles and responsibilities of the structures of the Company

The subjects involved in the process of combating money laundering and terrorism financing of the Company are:

1) Board of Directors, as the corporate body, which is responsible for:

- the establishment of the Anti - Money Laundering Function;
- the appointment, in consultation with the Shareholders, of the Anti - Money Laundering Officer;
- the approval of the Anti - Money Laundering and Terrorism Financing Policy and Organisational Model;
- implementation of the resolutions of the Board of Directors concerning the organisation, control and management of risk, including the risk of money laundering and terrorism financing, facilitating and disseminating at all Company's levels a risk culture;
- authorisation the exceptions of refrain from establishing relationships with individuals for whom the due diligence process has not been completed;
- authorisation of the start/continuation of a relationship with PEPs or other clients to whom a "high risk" class is assigned;
- acceptance the exceptions of refrain from establishing relationships with so called "Omnibus" accounts payable to trust companies and/or financial intermediaries;
- approval of the operating procedures that describe the activities to be undertaken in order to comply with anti - money laundering obligations;
- identifying the business functions/ relevant personnel delegated to the identification of Customers and formalising their assignments

2) the Control Function responsible for supervision of this activity is **Compliance and AML Officer,** who performs compliance audits, with intervals determined following its activity plan.

The Compliance and AML Officer shall communicate any violations of anti - money laundering rules in exercising its duties to the corporate bodies who are responsible for the assessment on possible necessity to report the case to the Supervisory Authority pursuant to the aforementioned Articles.

The Board of Directors of the Company has established the Anti - Money Laundering Function, which was located within the Compliance and AML Officer. The person appointed to the post of Anti - Money Laundering Officer of the Company is appointed by the Board of Directors, after internal consultation of the Board Members, in respect of the appointment, the individual is verified to have met the requirements of independence, authority, professionalism and integrity set out below:

Independence and authority requirements: the Anti - Money Laundering Officer must not have direct responsibility for operational areas in the field of AML or be

hierarchically dependent on individuals responsible for these areas and must have an adequate organisational positioning and contractual status.

Professional requirements: the post of Anti - Money Laundering Officer must be held by an individual having knowledge of the subject and of the relevant legislation, organisational structures aimed at preventing the risks of money laundering and related procedural models, as well as technical competencies and skills.

Integrity requirements: the role of Anti - Money Laundering Officer cannot be held by individuals who:

a) has not got qualifications in field professional legal advocacy, confirmed by granting the title of attorney at law or similar title in this respect, authorised by relevant legal association to perform legal advisory in the country of residence of the candidate for Anti - Money Laundering Officer

b) have been convicted in first instance:

- to imprisonment for one of the crimes provided for by the rules governing banking, financial, estate, insurance activities and the rules governing markets, securities and payment instruments;
- to imprisonment for a period not less than of one year for a crime against the public administration, against public faith, against property, against public order, against the public economy or for tax offences;
- to imprisonment for a period not less than two years for any unpremeditated crime

The tasks entrusted to the Anti - Money Laundering Officer of the Company are:

- to identify the applicable rules on the ongoing basis, with the support of industry associations, and to assess their impact on internal processes and procedures through or with the support of Management Boards of Collaborators or their General Partners - depending on the type of legal entity - evaluate their impact on internal Know Your Customer processes;
- to cooperate in identification of the Compliance and AML Control System and of the procedures/ guidelines aimed to preventing and countering AML / CTF risks and to propose organisational and necessary or appropriate procedural amendments in order to ensure adequate monitoring of risks;
- to check the suitability of the Compliance and AML Control System and the procedures adopted and propose the necessary and appropriate organisational and procedural amendments in order to ensure an adequate management of risks;
- to provide advice and assistance to the governing bodies and top management and, in case of new products and services offer, carry out preventive assessments on anti - money laundering topics, performing

preventive assessments of competence in case of new product and services offer;

- to manage relationships with Investigative Authorities;
- to check the reliability of the IT system providing data to the Centralised Electronic Archive;
- in case if it's required by the applicable law or by the contractual provisions, to transmit within due date to the relevant Financial Information Unit aggregated data concerning registrations in the Centralised Electronic Archive (CEA)
- to support performing enhanced Customer due diligence in cases of suspicion of money laundering and in any other case where the risk of money laundering seems particularly high also in relation to the Customer profiling according to money - laundering risk;
- to develop and treat the upgrade of a document (Anti - Money Laundering - Anti Terrorism Organisational Model) defining responsibilities, tasks and modes of operation in the money laundering and terrorism financing risk management, to be submitted for approval to the Board of Directors;
- to ensure, in coordination with other company functions competent in training, the preparation of an adequate training plan aimed at achieving an update on an ongoing basis for employees and collaborators;
- to periodically arrange the information flows to the corporate bodies and top management;
- to present to the Board of Directors and the Shareholders a report on actions taken, ascertained dysfunctions and related corrective actions as well as training activity for personnel;
- to cooperate with the competent authorities in investigations relating to the fight against money laundering and terrorism financing.

In order to fulfil these obligations, the Anti - Money Laundering Function:

- performs an AML / CFT self - assessment evaluation aimed at identifying the risks of money laundering and terrorism financing specific to each work process, checks the level of control on the those risks and identifies actions that can be put in place for their mitigation or management;
- operates independently and critically on the basis of an annual plan of activities approved by the Board of Directors, having unconditional and direct access to all business activities as well as to all data and necessary information;
- receives the maximum cooperation from all the other corporate and organisational structures to allow the full achievement of the objectives assigned to it and access to all Company activities and any relevant information to perform their tasks;
- has an organisational position that ensures its independence, authority and the possibility of direct reporting to the Board of Directors;

- reports annually, to Board of Directors on the steps taken, the ascertained dysfunctions and related corrective actions as well as training of personnel.

The staff called to cooperate with the Anti - Money Laundering Officer, even if working in other Departments/Organisational Units, reports directly to the AML Officer regarding the tasks pertaining to the Anti - Money Laundering Officer.

The Board of Directors has also attributed to the designated member of the Board of Directors as a Legal Representative responsible for the evaluation and transmission to the relevant Financial Information Unit of suspicious reports.

In terms of Reporting on Suspicious Transactions, the Anti - Money Laundering Officer is called to perform the following tasks:

- assessing and managing, in accordance with the procedures in place, the suspicious transaction reports received and transmit to the relevant Financial Information Unit those considered well - founded, upon the suspension of transactions;
- playing the interlocutor role in contacts with the relevant Financial Information Unit, providing answers to any requests for further study;
- authorising timely the communication to the relevant Financial Information Unit of suspected transaction in case of presence in the international anti - terrorism lists of names related to ongoing relationships with Customers, upon receipt from the competent Organisational Unit of written notice of the transactions block.

5.2. Roles and responsibilities of foreign Collaborators' structures

For each foreign Collaborator or their subsidiaries or branches) it is expected to identify a Local AML Compliance Officer - in the absence of an autonomous function or organisational unit - who, working in close functional coordination with the Anti - Money Laundering Officer of the Company, the Local Managerial Function (e.g. Management Board or General Partner) oversees the processes related to legislation on anti - money laundering within its respective jurisdiction.

The Local AML Compliance Officer or the Local Managerial Function shall:

- monitor the way of fulfilling the obligations of combating money laundering, terrorism financing, highlighting to respective corporate governing bodies or General partner(s), Anti - Money Laundering Officer at the Company and the competent structures any detected anomalies in the conduct of its activity;
- inform, in a complete and timely manner, the Anti - Money Laundering Officer of the Company, for matters of specific interest, the results of the control activities carried out by the supervisory authorities of the Company, as well as any significant occurrence.
- Depending on the cases, the Local Anti - Money Laundering Officer or the Local Managerial Function is also entrusted with the responsibility for evaluating and sending to the relevant regulatory authorities of the reports of suspicious transactions in terms of anti - money laundering/anti - terrorism, in accordance with the local legislation. In this context, this person the Local Anti - Money Laundering Officer, for which the coordination and control model applies, shall transmit to the Anti - Money Laundering Officer of the Company the copy of the report submitted to the competent Supervisory Authority, together with the grounds for such decision. The latter, for further study of abnormal operation transactions and relationships in the Group, can also make use of the collaboration of other functions of the foreign Collaborator.

The Local Anti - Money Laundering Officer or the Local Anti - Money Managerial Function is also required to provide the Anti - Money Laundering Officer of the Company with a continuous and regular flow of information, with particular reference to:

- changes in the risk profile attributed to Customers;
- authorisations granted for the start/continuation of the business relationship with Customers.

6. Risk management regarding money laundering and terrorism financing

Money laundering and terrorism financing risk management is entrusted to the internal procedures and information systems used by the Company.

In accordance with EU directives and national reference provisions treated as the guidelines, the Company considers the "*Customer insight*" an indispensable factor for an effective fight against money laundering and use of assets of illicit origin.

In this sense, the Company complies with the due diligence requirements concerning the Customer through:

- identification and verification of the identity of the Customer and the beneficial owner;
- the collection and the assessment of information about the scope and the nature of the ongoing relationship;
- constant control during the course of the business relationship, analysing the transactions concluded.

The activity of the Customer Due Diligence is also founded on the attribution of a risk profile, which provides different levels of authorisation depending on the degree of risk associated with the Customer.

The Customer Due Diligence requirements shall apply to all new Customers as well, upon this risk assessment, the Customers already acquired.

6.1. Risk management regarding money laundering and terrorism financing in the Company

The main checks foreseen at the level of procedures and systems adopted by the Company refer to the following activities:

- identification, Customer Due Diligence and record - keeping;
- registration in the Centralised Electronic Archive;
- recognition and reporting of suspicious transactions (“STR”).

The Customer identification activity is carried out by the dedicated personnel of the Company, while Customer Due Diligence is carried out by competent organisational units, before starting the relationship with a Customer.

In line with the risk - based approach, in compliance with applicable provisions of law, the evaluation model of the risk of money laundering and financing of terrorism is defined as a function of the type of Customer and the activities of the Company. Therefore, due diligence requirements are fulfilled measuring the risk associated with the type of Customer, the "ongoing relationship", transaction, product or transaction in question.

The data acquired in the performance of Customer Due Diligence obligations is recorded promptly and in any event no later than the thirtieth day following the completion of the transaction in respect of existing crypto currency account (either the major or minor period provided by applicable law), change and closure of the account, in the CEA of the Company in order to ensure retention of personal data and to enable any investigation of possible money laundering or terrorism financing by the Supervisory Authority or any other competent authority.

The registration of data in the CEA of the Company is managed by an IT process that includes automatic feeding system through the management applications.

6.2. Risk management regarding money laundering and terrorism financing of foreign Collaborators

Subject to compliance with specific requirements set out in the legislation of the host country, the procedures in place and information systems at the foreign Collaborators, as well their subsidiaries or branches are harmonised with the standards laid down by the Company and which will ensure the sharing of information, if its required.

To this end, the foreign Collaborators are required to implement the arrangements foreseen for the Company by this Policy, adapting them to their organisational context for the allocation of roles and responsibilities, subjecting them to the procedure for approval in order to issue specific set of internal rules. The International - wide strategic decisions regarding the risk management for money laundering and financing of terrorism shall be referred to the corporate bodies of the Company. The Corporate Bodies or General Partners of the foreign Collaborators should be aware of the choices made by the Company and are responsible, according to their skills, as part of the implementation of their own reality of the risk management strategies and policies for money laundering and financing of terrorism. In particular, each of the foreign Collaborators is responsible for its obligations related to:

- adequate knowledge of Customers (so called: "*Know Your Customer*");
- sending the data on anti - money laundering to the competent Supervisory Authority;
- reporting of suspicious transaction to the competent Supervisory Authority.

The latter must also cooperate with the competent structures of the Company in order to standardise as much as possible their methodologies and operational standards to the regulations issued by the Company.

7. Information flow

The Anti - Money Laundering Officer of the Company shall submit annually to the Board of Directors a report on the activities carried out by the same and by Local Anti - Money Laundering Officers and / or Local Managerial Function of foreign Collaborator under the relevant Anti - Money Laundering functions of the Company.

The Anti - Money Laundering Officer of the Company, also, provides the annual AML /CFT self - assessment activity to identify the risks of money laundering and terrorist financing of each work process, ensure the level of control over the same risks and identifies the actions that can be implemented to mitigate or management these risks. In addition, this subject provides an annual activity plan for each year.

In this scope, local Anti - Money Laundering Officers and / or local Anti - Money Laundering Referents of foreign entities adhere the drawing up of relevant compliance and AML documentation with the pattern applicable to the Company (annual report / annual activity plan / annual AML / CFT self - assessment) and share it with the Anti - Money Laundering Officer of the Company, before proceeding with its formalisation.

Also, at the request of the Board of Directors, the Anti - Money Laundering Officer of the Company is required to produce any documentation it deems necessary in order to give evidence of activities carried out.

For the purposes of the disclosure requirements listed above, Local Anti - Money Laundering Officers and / or Local Managerial Function of foreign Collaborator shall forward to the Anti - Money Laundering Officer of the Parent Company - in addition to the annual report / annual activity plan / annual AML / CFT self - assessment mentioned above - specific periodic information flows, and in particular:

a) a semiannual report that highlights:

- the activities carried out to check the risk of money laundering and terrorism financing and the main emerging evidence;
- details of the anti - money laundering/anti - terrorism risk profiles attributed to the clients;
- a list of names recognised by the anti - money laundering/anti - terrorism lists and evaluated as "false positives";

b) for the Annual Report on update representation of the activities and actions carried out under AML topics.