Customer Due Diligence Procedure for SimpleFX Ltd.

Approval Date:

27/10/2023

Type of approval/update

Approved upon the Resolution of Board of Directors

1. 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 Policy for preventing Money Laundering and Terrorism Financing SimpleFX.
5. **"Procedure"** shall mean Customer Due Diligence Procedure for SimpleFX Ltd.
6. "**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).
7. **"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.
8. **"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.).
9. "**Transaction"** shall mean any deposit, withdrawal, exchange or transfer of funds.
10. "**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.

11. **"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.
12. "**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.
13. **"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.
14. "**CFD account**" shall mean trading account and fund account collectively.
15. "**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.
16. "**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.

17. "**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.

2. Detailed model Customer due diligence.

Effective Customer Due Diligence/'Know Your Client' ("CDD") measures are essential to the management of money laundering and terrorist financing risk. CDD is identifying the Customer and verifying their true identity on the basis of documents, data or information obtained from a reliable and independent source both at the moment of starting a business relationship and on an ongoing basis.

Identification of Customer is coming to know Customer's identifying details, such as their name and address, his financial status and the capacity in which he is entering into the business relationship with the Company.

Verification is obtaining evidence satisfactory to the Company which supports this claim of identity.

The provisions hereunder shall implement the the rules and general provisions of Policy for preventing Money Laundering and Terrorism Financing SimpleFX ("Policy").

All terms used herein have the meanings given by the virtue of Procedure. Any other terms not defined in this document, the meaning of which does not result from the context in which they were used, have the meaning given by the virtue of the Policy. In case of any possible conflict between provisions hereof and thereof, the provisions hereof shall prevail.

2.1. Company's "Know Your Customer" approach.

For the purpose of the execution of CDD purposes, the Company shall:

- collect certain identification information from each Customer who opens an CFD account.
- utilise risk based measures to verify the identity of each Customer who opens an CFD account.
- record Customer identification information and the verification methods and results.

For all CFD accounts, if applicable, for any Natural Person or Legal Entity opening a new CFD account and whose name is indicated on the CFD account:

- Name, incorporation number, legal status, date and country of incorporation or registration (for Legal Entity).
- Date and place of birth (for Natural Person).
- A current address, which will be residential (for Natural Person) or registered office address and principal place of business (where different from the registered office - applicable to Legal Entity).
- Passport number and country of issuance, identification card number and country of issuance of any other government issued document evidencing nationality or residence and bearing colourful photograph constituting integrated and non-removable part of passport or identification card or other similar safeguard e.g. national identity cards, current valid passports or current valid driving licenses.
- The identity of underlying principles (including beneficial owners, controllers, directors or equivalent) with ultimate effective control over the capital or assets of an Legal Entity in addition to evidence that any Natural Person who purports to act on behalf of the Legal Entity is duly authorised and identify that person.
- The identify any Natural Person who exercises ownership or control over a Legal Entity, which are known as the beneficial owners. The indication and verification of beneficial owners, where relevant, extend to Legal Entity that own other Legal Entity, and the Company should look for the Natural Person(s) who ultimately exercises control through ownership or through other means of the Legal Entity that is the Customer. Control through other means may, inter alia, include the criteria of control used for the purpose of preparing consolidated financial statements, such as through a shareholders' agreement, the exercise of dominant influence or the power to appoint senior management. There may be cases where no Natural Person is identifiable who ultimately owns or exerts control over a Legal Entity. In

such exceptional cases, the Company, having exhausted all other means of identification, and provided there are no grounds for suspicion, may consider the senior managing official(s) to be the beneficial owner(s).

The bank transfer on Customers CFD account must be made from Customers bank account.

Where the underlying principles are not Natural Persons, The Company shall investigate further to establish the identity of the Natural Persons ultimately owning or controlling the business.

When opening an CFD account for a foreign Legal Entity, that does not have identification number, the Company will request alternative government issued documentation certifying the existence of the business or enterprise, including LEI number.

If a potential or existing Customer either refuses to provide the information described above or such information as the Company may require or appears to have intentionally provided misleading information, the Company shall not open a new CFD account and, after considering the risks involved, will consider closing any open CFD account(s) of an existing Customer.

Based on the risk, and to the extent reasonable and practicable, the Company will ensure that it has a reasonable belief that it knows the true identity of its Customers by using risk based procedures to verify and document the accuracy of the information received about the Customers. In verifying Customer identity, the Company will analyses any logical inconsistencies in the information obtained.

Customer's identity must be verified when:

- Establishing a business relationship with a new Customer,
- The Company suspects money laundering or terrorist financing,
- The Company has doubts about the veracity or adequacy of documents, data or information previously obtained for the purpose of CDD.

Where verification of identity is conducted after the establishment of the business relationship, verification will be completed as soon as is practicable after the business relationship has been established.

2.2. Methods of verification.

The Company shall verify Customer identity through documentary evidence and electronic verification (extraordinary means/ extraordinary verification). The Company shall use documents to verify Customer identity when appropriate documents are available. In light of the increased instances of identity fraud, the Company will supplement the use of documentary evidence by using the extraordinary means described below whenever possible. It may also use such extraordinary means, after using documentary evidence, if still uncertain about whether the true identity of the Customer is known.

In analyzing the verification information, the Company will consider, whether there is a logical consistency among the identifying information provided, such as the Customer's name, date of birth, street address and telephone number.

Appropriate documents for verifying the identity of Customers include, but are not limited to, the following:

- For Natural Person: a current government issued identification document evidencing nationality, residence, bearing a colorful photograph, constituting the integral, non-removable part of the document or similar safeguard, such as a driver's license, ID document or passport.
- For Legal Entity, documents showing the existence of the entity, such as:
    1) Certificate (Act) of Incorporation,
    2) Articles (Memorandum) of Association,
    3) Certificate of Incorporation,
    4) The last two years financial statements or three months of company bank statements,
    5) Copy of Register of Shareholders or a copy of Central Register of Companies and Partnerships, providing data related to the Shareholders,
    6) Copy of Register of Directors or a copy of Central Register of Companies and Partnerships, providing data related to the Directors,
    7) Individual verification of all active Directors,
    8) Individual verification of Shareholders/Beneficial Owners with a holding of 25% + 1 or more of Individual shareholders,
    9) a government issued business license (if applicable), etc.
- Said documents shall provide the following data required to properly identify the Legal Entity:
    a) legal form,
    b) country where it is registered,

c) the Authority responsible for the registration of the Legal Entity,
d) registration number,
e) its registered office,
f) the purpose of establishing the Legal Entity,
g) name and surname of management bodies,
h) other persons authorized to represent the Legal Entity and the scope of the authorization (if it's available),
i) beneficiary (beneficial owner).

The Company will not be required to take steps to determine whether the document that the Customer has provided for identity verification has been validly issued and it may rely on government issued identification as verification of a Customer's identity. If, however, it appears that the document shows some most probable as well obvious form of fraud, the Company will consider that factor in determining whether it can form a reasonable belief that it knows Procedure to the Customer's true identity.

To avoid any possibilities of providing the counterfeit document by the Customers, any identifying document (e.g. ID cards, passports and driving licenses in some jurisdictions) of each Natural Person shall meet the following requirements:

1. non-exchangeable and recognizable colorful head photo (the ID wherein the picture may be attached by third party is not suitable for identification),
2. the name of the Natural Person who is being identified,
3. date of birth of a Natural Person,
4. a signature of the Natural Person being identified - in case it is required by the applicable domestic law,
5. the Authority issuing the document

Considering the nature of the Company's business activity, where is not possible to submit an identity card personally, thus there are following methods to remotely assess the credibility of the identity documents submitted:

i. Using the Verified Electronic signature by Customer
ii. Sending the authorized copy of identifying document by the courier letter
iii. The identification is to be covered by the already existing bank account of Customer, where the bank has registered office or branch in a European Union Member State

iv. Online identification by the designed IT tool aimed at verification and biometric facial recognition to determine, whether the person on the other end of the transaction is who they say they are.
   a. To this end, the Customer shall upload his/ her picture made by IT tool, using Internet camera.
   b. The picture must present Customer's front of the whole face without any headwear.
   c. The Customer is required to make his/her picture in which he/she is holding a visible white sheet of paper, presenting the handmade or printed brand name of SimpleFX and current date.
   d. The personnel verify if the person in the uploaded picture is the same person like in the documents provided by him/her.
   e. In case of any doubts, the personnel ask for upload the another picture with the sheet of paper, presenting the handmade or typed the code designed by personnel.
   f. The code must contain at least one capital letter, number and special mark (e.g. $,#,%,*,&)

The Company will use the following extraordinary methods of verifying identity:

- Contacting a Customer.
- Independently verifying the Customer's identity through the comparison of information provided by the Customer with information obtained from reliable Internet source and/or other source.
- Checking references with other financial institutions or tax return as well declaration of income at least from previous financial year.
- Obtaining a financial statement.

Extraordinary methods of verification, strictly connected with the Enhanced Due Diligence, will be used in the following situations:

- When the Company is unfamiliar with the documents the Customer presents for identification verification.
- When there are other circumstances that increase the risk that the Company will be unable to verify the true identity of the Customer, as well beneficial owners in terms of the Legal Person through documentary means.

Should the Company reasonably believe that the true identity of a Customer cannot be established or the Company was misleading, it will do any or a combination of the following:

- Commence internal inquiry. Inquiry may require suspension of Customer's CFD account, which means that The Company may among others suspend Customers' orders including withdrawal orders up to 30 days.
- Not proceed with or terminate any business with the Customer.
- File a STR in accordance with applicable law and regulations.

2.3. Enhanced Due Diligence (EDD).

The regulatory measures requires further research and identification of Customers who may pose a high risk of money laundering to better assess the risks they pose.

If the Company has assessed that the business relationship or occasional transaction is a high risk relationship, based on the Customer's individual risk status, that is, the nature of the Customer, the business relationship, its location, or any other specificity of the business relationship, it will apply EDD measures. Except verification of source of funds, in case the thresholds, indicated in Article 8.5 hereof, are not exceeded, others EDD rules will be applicable to any transactions involving crypto currencies. By way of non-exhaustive examples, circumstances when EDD will be applied are:

- in case of the Company establishes a business relationship with a Customer from a country that has insufficient anti-money laundering and countering financing of terrorism systems or measures in place or;
- in case of a Customer seeks to conduct, through the Company, a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose the Company may in all circumstances consider that the level of risk involved is such that enhanced due diligence should apply to a particular situation;
- the amount of single transaction exceeds the thresholds indicated in Article 2.5 hereof.

In addition to CDD, the following enhanced requirements under EDD will apply:

a) Information relating to the source of the funds or the wealth of the Customer - without limitation in form of:
   - *i)* extract from bank account from current month;
   - *ii)* bill/ receipt/invoice indicated the payment in form of fiat currency or crypto currency;
   - *iii)* the contract/ agreement (with data anonymization regarding confidential and non-disclosure data) indicated the payment for goods or service in form of fiat currency as well crypto currency;
   - *iv)* employment contract with the remuneration granted by fiat currency as well crypto currency;
   - *v)* tax return;
   - *vi)* declaration of income;
   - *vii)* financial statement, especially prepared in line with the International Financial Reporting Standards (IFRS);

viii) extract of domestic Central Register of Companies and Partnerships, which contain the information concerning the approval of at least the annual financial statements by relevant authorities.

b) Carrying out more frequent and more extensive ongoing monitoring on the Customer and comparison with provided lists of terrorists and other criminals within openly accessible media sources (World-Check, reliable Internet source) will be conducted.

If suspicious information is found indicating possible money laundering or terrorist financing activity, the AML Compliance Officer shall file a STR in accordance with applicable law and regulations.

2.4. Politically Exposed Persons (PEP).

The Company will review public information, including information available on the Internet or in reliable databases, to determine whether any CFD account holders, are individuals who are or who have been entrusted with Prominent Public Functions, their Close Family Members or Persons known to be Close Associates ("**PEP**"), within the sense of meaning from definitions, indicated in Article 1 point 15-17 . If information indicating that an CFD account holder may be a PEP is found, and upon taking additional reasonable steps to verify this information, it is determined that the individual is, in fact, a PEP the Company will:

- Take enhanced due diligence measures to establish the source of funds and source of wealth of the PEP.
- Inform the AML Compliance Officer, who will assess the risk connected with the particular transactions related to PEP.
- Conduct enhanced ongoing monitoring of the business relationships involving the PEP.
- Establish or continue the business relationship only after prior Board of Directors approval upon the relevant resolution.

If suspicious information is found indicating possible money laundering or terrorist financing activity, the AML Compliance Officer shall file a STR in accordance with applicable law and regulation.

2.5. Monitoring CFD accounts for Suspicious Transactions.

The Company will monitor a sufficient amount of CFD account activity to permit the identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether FAFT designates particular jurisdiction as without limitation “High-risk and non-cooperative jurisdictions”, jurisdiction with imposed sanctions or (and) is involved, or any of the “red flags” identified below. The Company will look at transactions, including trading and wire transfers, in the context of other CFD account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that Customer.

The Company will identification of any suspicious activity and closely monitor any single transaction of amounted to or exceeding USD 10,000.00 (or equivalent) in terms of Natural Persons with the Non-European Union citizenship and Legal Entities established outside of the territory of European Union, or any single transaction equal or exceeding EUR 10,000.00 (or equivalent) with respect to every single transaction regarding to Legal Entities with the registered office or registered branch in the territory of European Union and Natural Persons with the EU citizenship.

The AML Compliance Officer will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious transactions to the appropriate authorities, when necessary.

Examples of suspicious transactions, behaviors or activities that should raise a "red flag" and cause further inquiry. These "red flags" may alert The Company employees to possible suspicious activity.

Some examples of "**red flags**" that could cause further investigation include:

- Customers who wish to maintain a number of trustee or CFD accounts that do not appear consistent with the type of business, including transactions involving nominee names.
- Matching withdrawals with deposits by different ways on the same or previous day.
- Exposure or abuse of transfers without completing trading operations on the CFD account.
- Revelation of unusual nature of operations that do not have obvious economic substance or obvious legal purpose.
- Customers who give conflicting information to different staff members.

- Large cash withdrawals from a previously inactive CFD account, or from an CFD account which has just received an unexpected large credit from abroad.
- Customer exhibits an unusual level of concern for secrecy, particularly with regard to the Customer's identity, type of business or source of assets.
- Legal Entity lacks general knowledge of its own industry.
- Customer is unconcerned with the risks, commissions or other costs associated with trading.
- Revelation of circumstances implying that the operations are performed for the purpose of money laundering or financing terrorism.

When a relevant personnel detects any "**red flag**", he must file an incident report without delay to the AML Compliance Officer, who may also be required to investigate the activity further under the direction of the AML Compliance Officer. This may include gathering additional information internally or from third party sources, classifying the CFD account as a high risk CFD account, placing the CFD account under heightened supervisory review, which includes, but is not limited to, depending on the situation, turning the CFD account over to the AML Compliance Officer for review of all orders prior to entry, daily review of all trading activity, review of all money transfer requests, review of all deposits, contacting the authorities, freezing the CFD account, or filing a STR. The Company shall not inform anyone outside of law enforcement or other competent authorities about a STR.

All above-mentioned rules shall be drawn upon the following steps:

- Proof of identity
- Proof of address
- Identification of data regarding to the account of a Legal Entity
- Proof of source of funds

2.6. Proof of identity

To provide the adequate identification of the Customer, the dedicated personnel shall act with the following rules aimed at mitigating the AML and terrorist financing risk.

1. In case the photo of the document, provided by the Customer, is
    a. blurry,
    b. blurred,
    c. all 4 corners of the document are invisible,
    d. black and white,
    e. photograph which is not constituting as an integrated and non-removable part of the document (the ID wherein the picture may be attached by third party is not suitable for identification)

The dedicated personnel shall go the step regarding to verification the proof of address and then send an email with the reason for the rejection of the document with the attached Verification Guide.

2. The personnel checks, whether the document does not come from a reserved country known as entered in national or international blacklists, sanction lists, embargo lists (UN, OFAC, Communitarian) and check it with relevant official websites (e.g. FATF website).
    A. without limitation the following countries are rejected: Iran, Mauritius, Myanmar, North Korea, Saint Vincent and the Grenadines, United States of America, Minor Outlying Islands (United States), Virgin Islands (U.S.).
3. The personnel investigates, whether a document is issued by the country in question and has all necessary elements.
4. The personnel checks, if the Customer is over 18 (note: some Asian countries with "shifted" years in the calendar).
5. The personnel verifies, whether the Customer is not PEP.
6. The personnel checks, if the Customer is indicated in the lists of terrorists and other criminals within openly accessible media sources (World-Check, reliable Internet source).
7. The personnel confirms, whether the document is still valid for a minimum of 3 months.
8. The personnel verifies, if the data indicated the Customer form as well on the provided document are the same, completed and visible.
9. In case of typos, then the personnel has to check, what needs to be changed in order for the data to be correct.

10. After accepting the document, we search for the client in the back office files and change its data to the correct one.
11. For Brazil, Mexico, Sweden, Canada, Australia, UK - The Company accepts driving licenses as proof of identity.
12. The personnel identifies biometric facial of Customer by the designed IT tool aimed at verification and determination, whether the person on the other end of the transaction is who they say they are.
13. The identification, specified in point 12 hereinabove could be replaced by:
    a. The already existing bank account of Customer, where the bank has registered office or branch in a European Union Member State;
    b. Using the Verified Electronic signature by Customer;
    c. Sending the authorised copy of identifying document by the courier letter.
14. In case of any misdoubt concerning nature of Customer the relevant personnel shall:
    a. Contact with a Customer.
    b. Independently verifying the Customer's identity through the comparison of information provided by the Customer with information obtained from reliable Internet source and/or other source.
    c. Checking references with other financial institutions (e.g. banks etc.)or tax return as well declaration of income at least from previous financial year.
    d. Obtaining a document involving proof of funds.
15. Should the Company reasonably believe that the true identity of a Customer cannot be established or the Company was misleading, the relevant personnel will do any or a combination of the following:
    a. Commence internal inquiry. Inquiry may require suspension of Customer's CFD account, which means that The Company may among others suspend Customers' orders including withdrawal orders up to 30 days.
    b. Not proceed with or terminate any business with the Customer.
    c. File a STR in accordance with applicable law and regulations.

2.7. Proof of address

The adequate identification of the Customer's address is strictly connected with the following rules aimed at mitigating the AML and terrorist financing risk.

1. If the Customer has sent an ID card / passport / ID card etc., we cannot accept this document as a proof of address, even if the document was issued less than 3 months ago.
2. The personnel repeats the steps, described in points 1 and 2 of Article 2.6 hereof.
3. The personnel investigates, whether the document was released no later than 3 months ago.
4. The Company examines, whether the Customer's details from the account are the same as those given in the Proof of identity steps, specified in Article 2.6 hereinabove.
5. The personnel investigates whether the issuer of the document actually exists (e.g., in case of an invoice, issued by a telecommunications company, the personnel checks the company's data and exemplary invoices in order to verify the correctness).
6. We check whether the customer's address provided on the invoice exists, if there is no exact address, we are searching based on the postal code.
7. For Russian and Ukrainian passports as a proof of address, the Company ask also to send an invoice or extract for bank account. The Company no longer accepts a page with a registered address in your passport as a proof of address.
8. The steps, specified in Article 2.6. point 14-15 hereof, shall apply accordingly.

2.8. Identification of data regarding to the account of a Legal Entity

Any Customer, acting in form of Legal Entity, regardless of its specified nature, shall upload a copy of following company documents in order to be positively verified:

1. Memorandum and Articles of Association
2. Certificate of Incorporation
3. LEI number
4. The last two years financial statements or three months of company bank statements
5. Copy of Register of Shareholders or a copy of Central Register of Companies and Partnerships, providing data related to the Shareholders
6. Copy of Register of Directors or a copy of Central Register of Companies and Partnerships, providing data related to the Directors
7. Individual verification of all active Directors
8. Individual verification of Shareholders/Beneficial Owners with a holding of 25%+ 1 or more of Individual shareholders

Any Customer, acting in form of Legal Entity, regardless of its specified nature, shall upload a copy of following company documents in order to pass the positive verification of its address:

1. A copy of a proof of a registered company address (e.g. utility bill, bank statement) not more than three months old is required in order to verify address. The document should, as a minimum, demonstrate the following information:
    a. Company Name
    b. Company Address
    c. Date of issue

The steps, specified in Article 2.6. point 1 a.-d. and Article 2.6. point 12 -15 hereof, shall apply accordingly.

2.9 Proof of source of funds

Identification of Customer's source of funds shall be implemented in mandatory or non-mandatory manner.

The non-mandatory identification of source of funds does not mean that it could be omitted based on someone's individual decision. Commencement that step is related to case by case study of each Customer and it's based on relevant personnel experience and its presentiments concerning her/his worries about the nature of particular Customer. In particularly non- mandatory identification of source of funds shall be initiate in following situations:

- The Company suspects money laundering or terrorist financing.
- The Company has doubts about the veracity or adequacy of documents, data or information previously obtained for the purpose of CDD.
- When the Company is unfamiliar with the documents the Customer presents for identification verification.
- When there are other circumstances that increase the risk that the Company will be unable to verify the true identity of the Customer, as well beneficial owners in terms of the Legal Person through documentary means
- other circumstances, defined in the Article 2.5 hereof as "the red flags"

The mandatory identification of source of funds shall be performed in the following circumstances:

1. in case of the Company establishes a business relationship with a Customer from a country that has insufficient anti-money laundering and countering financing of terrorism systems or measures in place or;
2. in case of a Customer seeks to conduct, through the Company, a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose the Company may in all circumstances consider that the level of risk involved is such that enhanced due diligence should apply to a particular situation;
3. the amount of single transaction exceeds the thresholds indicated in Article 2.5 hereof.

The documents which are deemed to be reliable proof of funds are indicated in Article 2.3 section a) point i. - viii. hereof.

The steps, specified in Article 2.6. point 1 a.-d. hereof, shall apply accordingly.

3.0. Storage of acquired Customers' data.

When transferring funds, the Company will record in its database at least the following information:

- The execution date of the transmittal order.
- The name and address of the recipient.
- The amount of the transmittal order.
- The identity of the recipient's financial institution.
- The CFD account number of the recipient.
- The documents provided by the Customers

For each transmittal order that the Company accepts, it will retain in its files any payment instructions received from the transmitter with the transmitter order and any form relating to the transmittal of funds that is completed by the person placing the transmittal.

All employees of the Company shall be aware of to whom and in what format their suspicions must be reported. They will also receive training from the AML Compliance Officer upon, and during the course of, their employment. The AML Compliance Officer shall hold AML records, STRs and supporting documentation confidential and ensure that STRs are filed as required. This information will not be communicated to anyone other than law enforcement or other competent authorities. After recognition the suspicious transaction, the **employee shall promptly** inform the AML Compliance Officer via e-mail about the transaction, clarifying its details and important circumstances connected with it (without limitation: situations considered to be ***red flags***, described in Article 2.5). **Once an internal suspicion report is made to the AML Compliance Officer or a STR has been submitted to the relevant supervisory authority, no employee of The Company shall warns or inform the owner of any funds of any report or any action that is to be taken in respect of any transaction concerning such funds.** When a STR has been made to the relevant supervisory authority with respect to a particular Customer, the Company shall ensure that due care is taken during subsequent enquiries so as not to alert the Customer about the disclosure. Appropriate measures (confidentiality of Company's employees; suspending of Customers withdrawals and deposits; reporting to the relevant Authorities, trainings for employees teaching them rules of non-tipping of confidential information and STRs etc.) shall be taken by The Company to ensure that the offence of tipping off is not committed.

As part of its AML program, The Company will maintain and keep documentation pertaining to Customer identity and verification for at least 5 years, for a period of five years after the end of a business relationship with their Customer or after the date of an occasional transaction.

4.0. Personnel.

The Company and the AML Compliance Officer shall ensure that employees are properly trained and are fully aware of the Company's AML/CFT policies and procedures. The Company will also perform criminal and disciplinary background checks on all employees before they are hired.

The Company will monitor its employees to ensure that AML procedures are adhered to. Based on the severity and nature of the violation, the employee will be reprimanded and warned that any future violation may result in termination. If the Company deems the violation to be intentional and or suspects the employee is involved in money laundering in any way, the employee will be terminated for cause without warning and reported to the relevant authorities.

The Company will develop ongoing employee training under the supervision of the AML Compliance Officer and senior management. The training will occur on an annual basis. It will be based on the Company's size, Customer base and resources. The Company will either develop the training program or contract for it.

On an annual basis, thereafter, the AML Compliance Officer will hold internal trainings for all employees. The training will include at a minimum:

- How to identify red flags and signs of money laundering that arise during the course of the employees' duties.
- What to do once the risk is identified.
- What employees' roles are in The Company's compliance efforts and how to perform them.
- The Company's record retention policy.
- The disciplinary consequences (including civil and criminal penalties) for non-compliance with the requirements of the applicable legislation.

The Company will review its operations to determine if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. The written procedures will be updated to reflect any such changes.

Employees must report any violation of the Company's AML/CFT compliance program to the AML Compliance Officer, unless the violation implicates the AML Compliance Officer, in which case the employee shall report the violation to senior management. Such reports will be confidential, and the employee will suffer no retaliation for making them.

5.0. Collaborator's "Know Your Customer" approach.

The Collaborator shall implement the Company's "Know Your Customer" approach model, which may be adhered to the requirements of the domestic law or particular business models as well corporate governance of each Collaborator. Until the Collaborator has not implemented its own AML Policy/ Procedure as well the local "Know Your Customer" approach model, the provisions hereof shall apply accordingly. In case of any conflict between the domestic binding law and provisions hereof, the domestic binding law provisions shall prevail.