AMEGA

KYC Policy

Effective June 8, 2021

This document describes Amega Markets LLC (hereafter the 'Company', 'Amega' or 'we') KYC policy and the procedures the Company has in place to identify, verify and monitor its Customers.

Know Your Client and Due Diligence

Before opening an account, we shall see to it that satisfactory and competent evidence is properly obtained on the identity of their customers and that effective procedures have been applied for such verification especially on new customers. Customer Account Information Form (CAIF) is kept for the customers.

Due diligence must be exercised to prevent the use of the Company as an instrument for money laundering. The Company implements the following procedures to become aware when it is being requested to "launder money":

- Customer identification: The Company will take all reasonable steps (exercise "due diligence") to establish, to their satisfaction, the true and full identity of each client, and of each client's source of wealth, financial situation and investment. Due diligence is essential for an individual with a high net worth whose source of funds is unclear. We will ensure that we are able to "know" at all times the identity of the persons with whom we are dealing;
- Customer's suspicious activity: If there are any suspicions about the activities (dealings, money transfers etc.) of an existing or potential customer, they should be reported immediately to the Compliance Officer, who will:
    - receive reports of suspicious activity from the Company's personnel
    - coordinate required AML reviews/meetings with appropriate staff
    - gather all relevant business information to evaluate and investigate suspicious activity
    - determine whether the activity warrants reporting to senior management ; and
    - design and implement training programs as required by this Policy.
- Employees are prohibited from disclosing to a client or any other person that information has been passed to the Compliance Officer, management or the regulatory authorities;
- To ensure compliance with this requirement, all personnel will be required to sign a statement on breach of confidentiality provision of the AML.

The Company can be exposed to reputational risk and should therefore apply enhanced due diligence to such operations. Private accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalized

investment company. In each case reputational risk may arise if the Company does not diligently follow established KYC procedures.

All new clients and new accounts are approved by at least one person, the Compliance Officer. In case of a new high-risk customer, the final decision is taken by the CEO. Particular safeguards have been put in place internally to protect confidentiality of customers and their business, the Company ensures that equivalent scrutiny and monitoring of these customers and their business is conducted, e.g. it is available to be reviewed by Compliance Officer and auditors.

The following are safeguards put in place to protect confidentiality of customers and their business:

- that employees will be required to sign confidentiality agreements
- that the Company will adhere to data protection laws
- that there will be segregation of duties between staff and departments and information will be available to different individuals on a need to know basis; and
- that the organization has put in place strong IT controls to ensure data safety.

Customer Identification

The identification of customers seeking to open an account with us is an essential part of our KYC process. The Company does not enter into any service relationship until the identity of the new customer or the person acting on his/ her behalf (Beneficial Owner) is fully verified. Information must be provided to learn:

- the true Identity of the Customer
- the nature of the Customer's Business; and
- the intended Purpose of the Customer's transactions.

The extent and nature of the information depends on the type of applicant and the expected size of the account.

Private customers (natural persons)

If the customer is a Natural person, the following information must be collected:

- true name and/or names used
- residence address, postal code, phone number; and
- date and Place of birth.

Names should be verified by:

- valid Passport
- national ID Card
- driving license; and
- Residence Permit.

The indicated documents should not be older than 6 months from the filing date.

The current permanent address will be verified by one of the followings:

- proof of a recent utility bill
- customer's tax identification numbers, Social Security number or Government Service and Insurance System number
- bank statement; and
- credit card monthly statement.

The utility bill, bank statement and credit card statement should not be older than 3 months from the filing date.

The copy of the customer's tax identification numbers, Social Security number or Government Service and Insurance System number should be apostilled in the country of origin.

For each account we shall also make reasonable effort, prior to the settlement of the initial transaction, to obtain the following information to the extent it is applicable to the account:

- occupation of customer
- the customer's investment objective and other related information concerning the customer's financial situation and needs; and
- annual income, Assets or net worth.

Approval of the Account or "new client" is subject to the following terms and conditions:

- the Customer Account Information Form is filled in completely
- clear copy of a valid ID with photo of the client is obtained
- recommendation of client is provided by the Investment Agent; and
- sufficient background check is conducted by our compliance team.

All applications are carefully examined by the compliance officer to ensure that all required information/ documents are gathered. To approve an application, the Compliance officer must verify the following:

- the completeness of the required agreement/identification documents

- the correctness, authenticity and completeness of the information provided by the applicant
- the creditworthiness of the applicant, through a database search whenever this deems necessary
- the probability that the applicant is involved in illegal or criminal activities; and
- and, reject all applications that do not include all the necessary information.

Enhanced Customer Due Diligence

Amega will perform enhanced customer due diligence:

- where a higher risk of money laundering or terrorist financing has been identified
- where through supervisory guidance a high risk of money laundering or terrorist financing has been identified
- where a customer is from a foreign country that has been identified by credible sources as having serious deficiencies in its anti-money laundering or counter terrorist financing regime or a prevalence of corruption
- in relation to correspondent banking relationships
- where the customer is a politically exposed person; or
- in the event of any unusual or suspicious activity.

High Risk Customers/ Politically Exposed Persons

A PEP is an individual entrusted with a prominent public function in the last three (3) years and includes any immediate family member or close associate of such an individual. Both local and foreign PEPs are covered by this definition.

The Company will have a risk management system in place to determine if prospective clients and prospective or existing customers are PEPs and should conduct regular searches and checks for this purpose.

The Company will search for information from reliable sources including https://www.world-check.com and google search. The Company will also rely on public information as allowed by the Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures in determining whether persons are within the definition of „close associates" (for example, partners or joint venturers), and will conduct regular searches and checks for this purpose.

Enhanced CDD and enhanced ongoing monitoring (on a risk-sensitive basis) are required whenever a customer, or any beneficial owner of a customer, is or becomes a politically exposed person (PEP). A “customer” for this purpose includes any

person entering a business relationship or undertaking a one-off transaction with the reporting entity.

If the customer is a high risk or politically exposed person, the Company will perform the following procedures:

- adequately identify the person and verify his or her identity as set out in this section
- have appropriate risk management systems to determine whether the customer is a politically exposed person
- obtain the approval of senior management before establishing a business relationship with the customer
- take reasonable measures to establish the person's source of wealth and source of property; and
- conduct regular enhanced monitoring of the business relationship.

Procedures when dealing with “Politically Exposed Persons”

When dealing with Politically Exposed Persons, Amega will perform the following procedures:

In addition to satisfying customer due diligence requirement we will:

- put in place risk management systems to determine whether a person or beneficial owner with whom that person has a business relationship is a politically exposed person, family member or close associate;
- ensure that the risk management procedures:
    - contain as a component, procedures for requiring that senior management approval be obtained before establishing or continuing a business relationship with a politically exposed person or a family member or close associate
    - take reasonable measures to establish the source of wealth and the source of funds of a person involved in a business relationship and a beneficial owner identified as a politically exposed person or a family member or close associate; and
    - contain as a component, monitoring of the business relationship with the politically exposed person or a family member or close associate.

KYC procedures for dealings with professional intermediaries and / or reseller clients

When dealing with intermediaries or third parties to undertake our obligations to introduce business, we will perform the following procedures:

- immediately obtain the information required
- ensure that copies of identification data and other relevant documentation relating to the requirements will be made available to it from the intermediary or the 'third party upon request without delay; and
- satisfy ourselves that the third party or intermediary is regulated and supervised for, and has measures in place to comply with the anti-money laundering procedures.

Changes to the Customer Status and Operations

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

- a material change in the way an account is operated, such as:
    - change of persons authorized to handle its account;
    - request for opening a new account in order to provide new investment services and/or financial instruments;
- a significant transaction that appears to be unusual and/or significant than the usual type of trade and profile of the client.

Enhanced Customer Scrutiny and Rejection

Based on the risk, we will analyze any logical inconsistencies in the information or behaviour of its customers. If a potential or existing client either refuses to provide the information described in the above chapters, or appears to have intentionally provided misleading information, a new account will not be opened and, after evaluating the risks involved, will consider closing any existing account. We will also refuse any account which is determined to be “high risk” by the Compliance officer.

Verification of Customer Identity

The Company has implemented an integrated multilevel electronic system of information verification provided by the Customer. This system documents and checks identification details of the Customer, keeps and controls drill through reports of all the transactions.

The following are some counter checks being done by us to verify identity of clients without face to face contact:

- telephone contact of the applicant at an independently verifiable home or business number
- submission of Income tax return, and also bank statement or any proof of income; and
- confirmation of address through correspondence or presentation of proof of billing address.

Above procedures should be strictly implemented when opening of accounts via telephone, internet or by mail; especially if the client is just referred by another client or any of the staff. Such requirements should ideally be done prior to executing the initial transaction. For non- residents who seek to procure transactions without face-to-face contact, documents as enumerated above issued by foreign authorities must be submitted.

The Company always requires its clients to submit information particularly on the source of funds. If the client states that he/she has a business, some proof of the business documents, like by-laws, Business registration, etc. are requested. Company search on the website for registered companies is done to ensure that the corporate or other business applicant is an existing business entity.

Customer identification and information of existing clients should be updated and/or amended at least once every two (2) years. This refers to change of residential or business address, new identification cards, new passport, additional business information, new business investment/venture, and the like. For any change of information before the said period the Company requests a letter or document pertaining to the changes being made.

Bearing in mind the “Know – Your – Customer” principle, we should be in a position of no- doubt or no suspicions that the identities of our clients are questionable after careful evaluation of all identification documents submitted to us. This should be very important where the client is a non-resident and therefore more probing must be done on the purpose of the transaction and the sources of funds, especially if it

involves a significant amount, except when such client is a long-established and well-known customer.

Once an account is opened for a client, particular care shall be taken in cases where instructions for transactions on behalf of said client are being made by another person or party, such person or party must be formally authorized by the client account to make such transactions on his/her behalf. The Company shall require the necessary documents such as Special Power of Attorney (SPA) or duly signature-verified authorization given by clients; e.g. authorized to place an order; up to what amount; and authorized to get the withdrawal.

We shall establish whether the applicant for business relationship is acting on behalf of another person as trustee, nominee or agent. The Company shall obtain authorized evidence of the identity of such agents (the same documents needed as enumerated above) and authorized signatories, and the nature of their trustee or nominee capacity and duties.

In cases where a potential customer insists for confidentiality reasons, a numbered account may be opened. Confidential numbered accounts should not function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence.

As a policy, we do not allow named account holders to transact for non-account holders and should therefore exercise special care and vigilance. Where transactions involve significant amounts, the customer should be asked to produce competent evidence of identity including nationality, the purposes of the transaction, and the sources of the funds.

The Company will document its verification, including all identifying information provided by the customer, the methods used and results of the verification.

Monitoring of Customer Activity

The Company monitors suspicious and revenue-intensive transactions closely, takes timely, appropriate actions on said transactions and informs the appropriate bodies without undue delay.

The system of monitoring implemented by the Company relies both on automated monitoring and, where appropriate, manual monitoring by the staff. A series of status

fields have been applied to customer accounts indicating their profile within the system, which assist automated monitoring. We have adopted a regulatory and legally compliant process for suspicious activity reporting that will enable all staff to make a report to the Compliance Officer where they know or suspect that a customer is engaged in money laundering or terrorist financing.

Our staff are trained to monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, type of transactions, geographic factors such as whether jurisdictions designated as “non-co-operative” are involved or any of the “red flags” identified below. The Company shall look at transactions, including deposits and wire transfer, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction for that customer. The Compliance Officer who will be responsible for this monitoring, will document when and how the transaction is carried out, and will report suspicious activities to the appropriate authorities.

Examples of Red Flags are:

- the Customer exhibits unusual concern regarding the Company’s compliance with government reporting requirements and AML Policy, particularly with respect to his/her identity, type of business and assets, or refuses to reveal any information concerning business activates, or furnishes suspicious identification documents
- the customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer’s stated business strategy
- the information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect
- upon request, the customer refuses to identify or fails to indicate any legitimate source for his/her funds and other assets
- the customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations
- the customer exhibits a lack of concern regarding risks, commissions, or other transaction costs
- the customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant to provide information, or is otherwise evasive regarding that person or entity
- the customer has difficulty describing the nature of his/her business or lacks general knowledge of his/her industry

- the customer attempts to make frequent or large deposits, insists on dealing only in cash equivalents, or asks for exemptions from the Company's policies relating to the deposits of cash and cash equivalents
- the customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to avoid the government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds
- for no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers
- the customer is from, or has accounts in, a country identified as a non-cooperative country by the Financial Action Task Force
- the customer's account has unexpected or sudden extensive wire activity, especially in accounts that had little or no previous activity
- the customer's account shows numerous currency or cashier's check transactions aggregating to significant sums
- the customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose
- the customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk
- the customer's account indicates large or frequent wire transfers, immediately withdrawn by check or by debit card without any apparent business purpose
- the customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose
- the customer makes a fund deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account
- the customer engages in excessive journal entries between unrelated accounts without any apparent business purpose
- the customer requests that a transaction be processed in such a manner to avoid the Company's normal documentation requirements
- the customer engages in transactions involving certain type of securities, such as penny stocks and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering. (Such transactions may warrant due diligence to ensure the legitimacy of the customer's activity); and
- the customer's account shows an unexplained high level of account activity with very low levels of transactions.

When a staff member of the Company detects any red flag he/she will investigate further under the direction of the Compliance Officer. This may include gathering additional information internally or from third party sources, contacting the appropriate authority or freezing the account.

Record Keeping

Records will be kept for all documents obtained for the purpose of customer identification (KYC Policy requirements) and all data of each transaction, as well as other information related to money laundering matters in accordance with the applicable anti-money laundering laws/regulations. That includes files on suspicious activity reports, documentation of AML account monitoring, etc.

Transaction effected via the Company can be reconstructed, from which the authorities will be able to compile an audit trail for suspected money laundering, when such a report is made to it. The Company can satisfy within a reasonable time any inquiry or order from the authorities as to disclosure of information, including without limitation whether a particular person is the customer or beneficial owner of transactions conducted through the Company. The following document retention periods will be followed:

- all documents in opening the accounts of clients and records of all their transactions, especially customer identification records, shall be maintained and safely stored for seven (7) years from the dates of transactions;
- with respect to closed accounts, the records on customer identification, account files and business correspondence, shall be preserved and safely stored for at least seven (7) years from the dates when they were closed.

The following records must be kept:

- copies of the evidential material of the customer identity
- any non-documentary verification methods or additional methods used to verify
- relevant evidential material and details of all business relations and transactions, including documents for recording transactions in the accounting books (the form and source of funds and/or securities used by the applicant for business; the form and destination of funds paid or delivered to the applicant for business or another person on his behalf; financial transactions carried out by the Company with or for each client or counterparty of the Company
- relevant documents of correspondence with the customers and other persons with whom they keep a business relation; and

- description of how the Company resolved all substantive discrepancies.

Checking and review of the documents is done by the personnel assigned to verify the accuracy and completeness of the records maintained by the Company. It is important that any material irregularity or documents lacking are noted and reported for immediate correction.

Transaction documents may be retained as originals or copies, on microfilm, or in electronic form, provided that such forms are admissible in court.

If the records relate to on-going investigations or transactions that have been the subject of a disclosure, they shall be retained beyond the stipulated retention period until it is confirmed that the case has been closed and terminated.