

ANTI-MONEY LAUNDERING, COUNTER TERRORIST FINANCING & KNOW YOUR CLIENT POLICY

Purpose

The purpose of this policy is to provide guidance on the Anti-Money Laundering, Counter Terrorist Financing and Know your Client Policy which is followed by the XGLOBAL FX Ltd. (“the Company”) in order to achieve compliance with the relevant anti-money laundering and counter terrorist financing (“AML/CFT”) legislation.

Legal Framework

Investment Firms in Cyprus are required to comply with the provisions of The Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007 to 2021 (the “Law” for the purposes of this policy) and the Directive for the prevention and suppression of money laundering and terrorist financing. The main purpose of the Law is to define and criminalize the laundering of proceeds generated from all serious criminal offences aiming at depriving criminals from the profits of their crimes. While XGLOBAL FX Ltd is regulated outside of Cyprus it follows the same procedures since its parent and sister company are domiciled and regulated in Cyprus.

In addition to recognising the vital importance of taking action to combat the financing of terrorism, the Company follows the guidelines set out by Authorities such as the FATF which set out the framework to detect, prevent and suppress the financing of terrorism and terrorist acts.

In accordance with the Law, Investment Firms are obliged to set out policies and procedures for preventing AML/CFT activities. Those procedures, which are implemented by the Company, as these are requested by the Law, are the following:

- a. Identification and due diligence procedures of clients.
- b. Record keeping procedures in relation to clients’ identity and their transactions.

- c. Internal reporting procedures to a competent person (e.g. Anti-Money Laundering Compliance Officer) appointed to receive and consider information that give rise to knowledge or suspicion that a client is engaged in money laundering activities.
- d. Appropriate procedures of internal control, risk management, with the purpose of preventing AML/CFT activities.
- e. The detailed examination of every transaction that due to its nature is considered vulnerable to money laundering, and especially for complicated or unusually large transactions and transactions that are taken place without an obvious financial or legal purpose.
- f. Measures for making employees aware of the above-mentioned procedures to prevent AML/CFT and of the legislation relating to AML/CFT.
- g. Provision of regular training to their employees in the recognition and handling of transactions suspected to be associated with money laundering.

Policy

The provisions of the Law have been adopted by the Company, which introduces procedures and processes that ensure compliance with the Law and Directives issued by its regulator on this matter.

1. CLIENT IDENTIFICATION AND DUE DILIGENCE PROCEDURES

The Company has adopted all requirements of the Law in relation to client identification and due diligence procedures. The client categorization, identification and due diligence follows a risk based approach where the Company implements a scoring system to categorize clients as:

- low risk,
- normal risk,
- high risk, such as but not limited to
 - i. Non face to face customers
 - ii. Accounts in the names of companies whose shares are in bearer form

- iii. Trusts Accounts
- iv. 'Client accounts' in the name of a third person
- v. 'Politically exposed persons' accounts
- vi. Electronic gambling /gaming through the internet
- vii. Customers from countries which inadequately apply FATF's recommendations
- viii. Cross-frontier correspondent banking relationships with credit institutions – Clients from third countries
- ix. Any other Clients that their nature entail a higher risk of money laundering and terrorist financing
- x. Any other Client determined by the Company itself to be classified as such.

Due diligence procedures are applied Prior to the establishment of a business relationship and further due diligence may be undergone at the Company's discretion, for example:

- there is a suspicion of money laundering or terrorist financing, irrespective of the amount of the transaction.
- there are doubts about the veracity or adequacy of previously obtained client identification data.
- the risk score of the client based on the Risk based approach of the Company

Failure or refusal by a client to submit the requisite data and information for the verification of his/her identity and the creation of his/her economic profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the client is involved in money laundering or terrorist financing activities. In such an event, the Company does not proceed with the establishment of the business relationship and considers the necessity whether the anti-money laundering officer is required to report to the VFSC.

When the account is opened, it is closely monitored. A review is carried out and a note prepared summarizing the results of the review, which are kept in customer's file and at frequent intervals, the Company compares estimated against the actual turnover

of the account. Any serious deviation, is investigated, for possible action by the Company in relation to the particular account concerned.

The practice to which the Company adheres in order to comply with the requirements of the Law on the subject of the client identification is achieved on a risk-based approach and it is set out below:

➤ *Client Due Diligence Procedure*

Client Due Diligence procedure shall comprise the following:

- i. Identification of the client and verification of the client's identity on the basis of information obtained from a reliable and independent source.
- ii. Identification of the beneficial owner and taking risk-based and adequate measures to verify his/her identity on the basis of documents, data or information issued by or received from a reliable and independent source. As regards to legal persons, trusts and similar legal entities, taking risk-based and adequate measures to understand the ownership and control structure of the client.
- iii. Obtaining information on the purpose and intended nature of the business relationship.
- iv. Conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the data and information held by the firm in connection with the client.

➤ *Timing of identification*

Client and beneficial owner identification occurs before the establishment of a business relationship, given that the Company prohibits any client's transaction or trade before the necessary documentation and information is provided.

➤ *Renewal of client identification*

Reviews of existing records take place on a regular basis, thus ensuring that the documents, data or information held are kept up-to-date. Client due diligence procedures are applied not only to all new clients but also at appropriate times to existing clients on a risk sensitive basis.

Simplified Client Due Diligence

Simplified procedures may apply for lower risk clients. More detailed client due diligence measures for lower risk clients shall apply when there is no suspicion of money laundering, regardless of any derogation, exemption or threshold, and not whenever a business relationship is established.

It should be noted that the Company shall gather sufficient information to establish if the client qualifies to be classified as lower risk client.

Enhanced Client Due Diligence

The Company should apply enhanced client due diligence measures in situations which by nature can present high risk of AML/CFT.

More specifically, where the client has not been physically presented for identification purposes, the Company shall take specific and adequate measures to compensate for the high risk, by applying measures such as:

- Ensuring that the client's identity is established by additional documents, data or information.
- Supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution.
- Ensuring that the first payment of the operations is carried out through an account opened in the client's name with a credit institution.

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country and close associate is someone with a close relationship with the political exposed persons.

The following additional due diligence measures to determine whether a prospective client is a politically exposed person:

- Approval from Senior Management prior to the establishment of a business relationship with the client.
- Take appropriate measures for the establishment of the origin of the client's assets and the source of funds that are related with the establishment of the business relationship or transaction.
- Conduct enhanced and continuous monitoring of the business relationship.

Anonymous or Numbered Accounts

The Company is prohibited from keeping anonymous or numbered accounts. Additionally, the Company shall pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favor anonymity and take measures to prevent their use for money laundering or terrorist financing purposes.

Due Diligence Performance by Third Parties

The Company is permitted to rely on third parties to meet the requirements for client due diligence. However the ultimate responsibility for meeting those requirements shall remain with the Company which relies on the third party.

Record keeping procedures

The Company should keep the following documents and information for use in any investigation into, or analysis, of possible money laundering or terrorist financing by national authorities:

- The name and address of clients and copies or records of official identification documents (like passports, identity cards, or driving licenses).
- The name and address (or identification code) of counterparties.
- The form of instruction or authority.
- The account details from which any funds were paid.
- The form and destination of payment made by the business to the client.
- Business correspondence.

For client due diligence, a copy of the references of the evidence is required, for a period of at least 5 years after the business relationship with the client has ended.

For business relationship and transactions, the supporting evidence and records for a period of at least five years following the carrying out of the transactions or the end of the business relationship.

The retention of the documents/data, other than the original documents or their certified true copies that are kept in a hard copy form, may be in other forms, such as electronic form, provided that the Company is able to retrieve the relevant documents/data without undue delay and present them at any time, to the VFSC, after a request. A true translation is attached in the case that the documents/data are in a language other than Greek or English.

Compliance officer report to VFSC

The employees' reports are evaluated by the Compliance Officer and if it is considered necessary the Compliance Officer notify the VFSC. After the submission of a suspicious report the customers' accounts concerned as well as any other connected accounts are placed under the close monitoring of the Compliance Officer. After submitting the suspicious report, the Financial Organisation adheres to any instructions given by VFSC and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active. Furthermore, after the submission of a suspicious report the customers' accounts concerned as well as any other connected accounts are placed under the close monitoring of the compliance officer.

Transactions executed for the customer are compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the customer and the data and information kept for the customer's economic profile. Significant deviations are investigated and the findings are recorded in the respective customer's file. Transactions that are not justified by the available information on the customer, are thoroughly examined so as to determine whether suspicions over money

laundering or terrorist financing arise for the purposes of submitting an internal report to the compliance officer and then by the latter to VFSC.

All necessary measures and actions must be taken based on the investigation findings, including any internal reporting of suspicious transactions/activities to the compliance officer.

Suspicious Transactions

The definitions of a suspicious transaction as well as the types of suspicious transactions which may be used for money laundering and terrorist financing are almost unlimited. A suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Financial Organisation has created for the customer. The Financial Organisation ensures that maintains adequate information and knows enough about its customers' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.

A list containing examples of what might constitute suspicious transactions/activities related to money laundering and terrorist financing are:

A. MONEY LAUNDERING

1. Transactions with no discernible purpose or are unnecessarily complex.
2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the customer.
3. The transactions or the size of the transactions requested by the customer do not comply with his usual practice and business activity.
4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the customer's business activities would not appear to justify such activity.
5. The business relationship involves only one transaction or it has a short duration.

6. There is no visible justification for a customer using the services of a particular Financial Organisation. For example the customer is situated far away from the particular Financial Organisation and in a place where he could be provided services by another Financial Organisation.
7. There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).
8. There are frequent small purchases of a particular financial instrument by a customer who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the customer's instructions, in an account other than his usual account.
9. Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.
10. Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.
11. The settlement of any transaction but mainly large transactions, in cash.
12. Settlement of the transaction by a third person which is different than the customer which gave the order.
13. Instructions of payment to a third person that does not seem to be related with the instructor.
14. Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on money laundering and terrorist financing.
15. A customer is reluctant to provide complete information when establishes a business relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with Financial Organisations, names of its officers and directors, or information on its business location. The customer usually provides minimum or misleading information that is difficult or expensive for the Financial Organisation to verify.

16. A customer provides unusual or suspicious identification documents that cannot be readily verified.
17. A customer's home/business telephone is disconnected.
18. A customer that makes frequent or large transactions and has no record of past or present employment experience.
19. Difficulties or delays on the submission of the financial statements or other identification documents, of a customer/legal person.
20. A customer who has been introduced by a foreign Financial Organisation, or by a third person whose countries or geographical areas of origin do not apply or they apply inadequately FATF's recommendations on money laundering and terrorist financing.
21. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).
22. The stated occupation of the customer is not commensurate with the level or size of the executed transactions.
23. Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.
24. Unexplained inconsistencies arising during the process of identifying and verifying the customer (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).
25. Complex trust or nominee network.
26. Transactions or company structures established or working with an unneeded commercial way. e.g. companies with bearer shares or bearer financial instruments or use of a postal box.
27. Use of general nominee documents in a way that restricts the control exercised by the company's board of directors.

28. Changes in the lifestyle of employees of the Financial Organisation, e.g. luxurious way of life or avoiding being out of office due to holidays.
29. Changes the performance and the behavior of the employees of the Financial Organisation.

B. TERRORIST FINANCING

1. Sources and methods

The funding of terrorist organisations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding “protection” money), smuggling, thefts, robbery and narcotics trafficking. Legal fund raising methods used by terrorist groups include:

- i. collection of membership dues and/or subscriptions,
- ii. sale of books and other publications,
- iii. cultural and social events,
- iv. donations,
- v. community solicitations and fund raising appeals.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of financial instruments, wire transfers by using “straw men”, false identities, front and shell companies as well as nominees from among their close family members, friends and associates.

2. Non-profit organisations

Non-profit and charitable organisations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organisations can be made in the following ways:

- i. Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.

- ii. A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.
- iii. The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.
- iv. The non-profit organisation provides administrative support to the terrorist movement. Unusual characteristics of non-profit organisations indicating that they may be used for an unlawful purpose are the following:
 - a) Inconsistencies between the apparent sources and amount of funds raised or moved.
 - b) A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.
 - c) A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.
 - d) Large and unexplained cash transactions by non-profit organisations.
 - e) The absence of contributions from donors located within the country of origin of the non-profit organisation.

2. CLIENT ACCOUNT OPENING PROCEDURES

Upon the initial client meeting the necessary due diligence procedures, as described above, are applied to ensure all Know Your Client (KYC) policies are adhered to, all documents necessary for proceeding with KYC procedure are provided and the Company may accept the client and proceed to the account opening. Subsequently the client completes the account opening forms indicating all required information. The responsible administrator collects all initial information of the client and forwards it directly to Senior Management and to the Anti-Money Laundering Compliance Officer for examination, review and approval. Following the approval, the administrator records all necessary information into the Company's software systems and communicates it to the related departments.

The minimum data of information that are collected before the establishment of the business relationship, with the aim of constructing the customer's economic profile should include the following:

- a) the purpose and the reason for requesting the establishment of a business relationship
- b) the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments
- c) the customer's size of wealth and annual income and the clear description of the main business/professional activities/operations

XGLOBAL FX Ltd collects and verifies the personal identification information of all account holders, and then subsequently logs and tracks the transactions that are carried out by its clients.

In order to open an account with XGLOBAL FX Ltd, a valid form of government issued identification (Passport, State ID, or Driver's License), a proof of residence, and bank account information is required, along with a completed account application.

It should be noted that XGLOBAL FX Ltd tracks any suspicious transactions made by clients and any transactions executed under non-standard trading conditions.

- XGLOBAL FX Ltd carries out its activities in line with the anti-money laundering framework as laid out by the Financial Action Task Force.
- All XGLOBAL FX Ltd client funds are held in separate, segregated accounts that are designated solely for client deposits and withdrawals.
- XGLOBAL FX Ltd monitors funding from bank accounts held outside the account holder's home country.
- XGLOBAL FX Ltd does not accept deposits from third-parties nor cash deposits or disbursements under any circumstances.
- XGLOBAL FX Ltd matches each deposit to the account name held on file for that customer.
- XGLOBAL FX Ltd reserves the right to refuse to process a transaction where it believes the transaction to be connected in any way to money laundering or criminal activity. In accordance with international law, XGLOBAL FX Ltd is

under no obligation to inform the client when suspicious activity is reported to any corresponding regulatory or legal bodies.

The “Financial Action Task Force” (FATF) sets AML policies for countries to follow. XGLOBAL FX Ltd is required to do an “Enhanced Due Diligence” on clients from the others as they are classed as High Risk by the FATF, thus, we cannot accept clients from The United States, North Korea, Iran, Myanmar, Cuba, Sudan, Syria and British Columbia in Canada including US citizens residing outside the US.

3. ACCOUNT OPENING REQUIREMENTS

“XGLOBAL FX Ltd is committed to the prevention of money laundering activities through our services and as such comply with regulatory requirements such as:

- Identifying our clients;
- Identifying, monitoring and reporting any kind of suspicious transactions; o Maintaining transaction records for minimum 5 years after the termination of our contractual relationships with our clients;
- Training our staff to recognize suspicious transactions and to fulfil all reporting obligations;
- Depending on client location, report any suspicious activities to authorities in several countries.”
 - Photo ID (*Please note that all photo IDs are verified through third-party compliance software.*)
 - A valid passport
 - A valid National Identity Card
 - A valid government ID, such as a Driver's License or State ID
 - Proof of Residence (*Please note that proof of residence must be current i.e. not older than 90 days*)
 - A utility or phone bill
 - A bank statement

Bank Account Requirements

- XGLOBAL FX Ltd account holders must have a valid bank or credit card account in their name. The bank/credit card statement must show their name and the same registered address as that shown on their application.

4. FUNDS WITHDRAWAL PROCEDURE

The withdrawal procedure at XGLOBAL FX Ltd detailed below follows the strict principle that ensures funds are securely remitted back to their originating source.

- XGLOBAL FX Ltd customers must complete a signed paper or digital withdrawal request containing inter alia, their correct account information.
 - The withdrawal form must be submitted to the XGLOBAL FX Ltd Back-office department for processing. The Back-office department will confirm the account balance, verify that there are no holds or withdrawal restrictions on the account, and then approve the withdrawal request, pending compliance approval.
 - The XGLOBAL FX Ltd Internal Reporting and Matching department reviews all withdrawal requests approved by the Back-office department, verifying that the original funds are being withdrawn through the same method of deposit and to the name of the account holder on file.
 - The Compliance department will also examine the withdrawal request against the customer's deposit history to ensure there is no suspicious activity, and if none verifies the bank account details held on file.
- Withdrawal requests approved by the XGLOBAL FX Ltd Compliance department are sent back to the Internal Reporting and Matching department, and the funds are released to the client.
- In the event that a withdrawal is flagged for suspicious activity, the withdrawal is placed on hold, pending further investigation by XGLOBAL FX Ltd management.
- XGLOBAL FX Ltd Management will decide if further action is needed and which, if any, relevant regulatory bodies need to be contacted.

5. MONITOR AND REVIEW

The Company will, on a regular basis, monitor and assess the effectiveness of this Policy and the sequence of its order execution arrangements and, in particular, the execution quality of the procedures explained in the Policy in order to deliver the best possible result for the Customer, and, where appropriate, the Company reserves the right to correct any deficiencies in this Policy and make improvements to its execution arrangements.

In addition, the Company will review the Policy as well as its order execution arrangements at least annually. A review will also be carried out whenever a material change occurs that affects the ability of the firm to continue to obtain the best possible result for the execution of its Customer orders on a consistent basis using the venues included in this Policy.

The Company will notify any Customers affected by material changes in its Policy or order execution arrangements.

6. COMPLIANCE FOOTNOTE

The compliance procedure related to AML listed above is only a brief summary of the compliance function guidelines followed by the XGLOBAL FX Ltd compliance team. A detailed copy of our compliance policy is available for qualified institutions, regulatory bodies, and related counterparties. For additional questions concerning XGLOBAL FX Ltd policies, please contact our Compliance department. No substitutions or modifications will be accepted to the requirements above. The XGLOBAL FX Ltd Compliance department reserves the final determination regarding the validity of these documents.

Clients should assume that all information provided to the Company is available to the competent regulatory authorities in (a) the country of incorporation of the Company, i.e. the Republic of Cyprus; (b) the country of origin of any funds transmitted to XGLOBAL FX Ltd; and (c) the destination country of any funds refunded by or withdrawn from the Company.

XGLOBAL FX Ltd does not want your business if your funds are sourced from criminal activities or if the nature of your account transactions is illegal in any manner whatsoever.

The Company reserves the right to review and/or amend its Money Laundering Prevention Policy, at its sole discretion, whenever it deems fit or appropriate.

Our AML Policy is a policy only, it is not part of our Terms and Conditions of Business and is not intended to be contractually binding.