MultiFi

MultiFi International Ltd

MONEY LAUNDERING & TERRORIST FINANCING PREVENTION POLICY

AML & CFT Policy

MultiFi

Table of Contents

MultiFi

1. INTRODUCTION

1.1. 'www.multifi.trade' is a domain owned and operated by MultiFi International Ltd, a company registered in Mauritius with company registration number C222494, having its registered office at Pope Hennessy Street, Suite 803, 8th Floor, Hennessy Tower, Port Louis, Mauritius (the "Company").The Company is regulated by the Financial Services Commission ('FSC') of Mauritius as a Securities Dealer with License number: GB22200883.

1.2. The Company is regulated by the Financial Services Commission (FSC) of Mauritius and holds a Global Business Licence and an Investment Dealer (Full Service Dealer, excluding Underwriting) Licence under Licence Number G825204228.

2. THE PURPOSE OF THIS POLICY

2.1. In its role as a regulated Securities Dealer, the Company is required to abide by the anti-money laundering (AML) and Counter Terrorism Financing legislation and regulations applicable in Mauritius (the "AML & CFT Laws and Regulations" – see further below), which apply to all of its activities, and has a duty to safeguard its customers' money.

2.2. In line with the foregoing, the principal objective of this Policy is to provide the Company's (prospective) Clients with a summary of the obligations of the Company in relation to complying with the applicable AML & CFT Laws and Regulations.

2.3. A comprehensive set of internal policies and procedures have been designed to assist the Company and its officer's, staff, agents and third party outsourced service providers in complying with the requirements of the relevant AML & CFT Laws and Regulations in order to prevent the Company from being used by money launderers to further their illicit business, is set out in the Company's "Manual for the Prevention of Money Laundering and Terrorist Financing".

3. OVERVIEW OF REGULATORY FRAMEWORK

3.1. As a regulated Securities Dealer, the Company is, *inter alia*, required to comply with the international and Mauritius laws and regulations pertaining to the prevention of money-laundering and terrorist financing, including, without limitation, the following:

MultiFi

A. AML/CFT Laws and Regulations

a. Anti-Money Laundering and Countering the Finance of Terrorism Act 2020;

b. Anti-Money Laundering and Countering the Finance of Terrorism Regulations 2020;

c. Anti-Money Laundering and Countering the Finance of Terrorism Regulations 2020 (1st Amendment);

d. Anti-Money Laundering and Countering the Finance of Terrorism Regulations 2020 (2nd Amendment);

e. Anti-Money Laundering and Countering the Financing of Terrorism (Amendment) Act, 2021;

f. Anti-Money Laundering and Countering the Financing of Terrorism (Second Amendment) Act, 2021;

g. Anti-Money Laundering and Countering the Financing of Terrorism (Amendment) Regulations 2022;

h. Anti-Money Laundering and Countering the Financing of Terrorism (National Risk Assessment) Regulations 2022;

i. Anti-Money Laundering and Countering the Financing of Terrorism (counter- measures) Regulations 2022;

j. Anti-Money Laundering and Countering the Financing of Terrorism (Cross Border Declaration) Regulations 2022.

B. Beneficial Ownership (BO) Identification Laws and Regulations

a. Beneficial Ownership Act 2020;

b. Beneficial Ownership Regulation 2020;

c. Beneficial Ownership (Amendment) Act, 2021.

C. Counter-Terrorist Financing Laws and Regulations

a. Prevention of Terrorism Act 2004;

b. Prevention of Terrorism (Implementation of UNSCR on Suppression of Terrorism) Regulations 2015;

c. Prevention of Terrorism (Amendment) Act, 2021;

d. Prevention of Terrorism (Second Amendment) Act 2021;

e. Prevention of Proliferation Financing Regulations, 2021;

f. Prevention of Terrorism (Implementation of United Nations Security Council Resolutions on Suppression of Terrorism) (Amendment) Regulations, 2022;

g. Prevention of Proliferation Financing (Amendment) Regulations, 2022;

D. FSA Guidelines, FATF Recommendations and IOSCO Principles

3.2. The above-mentioned laws and regulations are further complemented by set of industry guidance notes, the provisions of which the Company aims to incorporate into its policies, procedures, and day-to-day operations; as such, in addition to the above-mentioned laws and regulations, the Company is adhering to the following guidance documents:

a. Representative Application Guidelines;

b. Securities Dealer Application Guidelines;

c. Financial Action Task Force (FATF) Recommendations, which are recognized as the international standard for combating money laundering and the financing of terrorism and proliferation of weapons of mass destruction;

d. Any other relevant legislations and general rules and principles issued by the International Organization of Securities Commissions (IOSCO).

E. International Sanctions Regime

3.3. Finally, there is a separate but related 'International Sanctions Regime' that imposes restrictions on the Company's ability to do business with certain persons and entities on UN, United States (US) and European Union (EU) sanctions lists.

3.4. Some entries on these lists are specific to a particular person or entity and others are general financial sanctions on all persons and entities in a particular jurisdiction.

4. CRIMINAL OFFENCES

4.1. It should be noted that, under the above-mentioned laws and regulations, a number of different criminal offences may be committed, which are is punishable by prison sentences and/or fines, including, without limitation:

A. The offence of '<u>money laundering</u>'[1], which is punishable:

(i) For a natural person:

- with a fine not exceeding Rs 5,000,000; or
- imprisonment for a term not exceeding 15 years; or
- both such fine and term of imprisonment;

(ii) For a legal entity:

- with a fine not exceeding Rs 10,000,000

B. The offence of 'tipping off[2]', which is punishable:

- with a fine not exceeding Rs 5,000,000; or
- imprisonment for a term not exceeding 10 years; or
- both such fine and term of imprisonment;

C. The offence of 'misrepresentation'[3], which is punishable:

- with a fine not exceeding Rs 10,000,000; or
- imprisonment for a term not exceeding five years; or
- both such fine and term of imprisonment;

D. The offence of 'malicious reporting'[4], which is punishable:

- with a fine not exceeding Rs 200,000; or
- imprisonment for a term not exceeding six years; or
- both such fine and term of imprisonment;

1 '*Money Laundering*' occurs where a person knowingly or having reasonable grounds to suspect that an asset, in whole or in part, directly or indirectly represents proceeds of crime:

a) converts or transfers that property for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his action;
b) conceals or disguises the true nature, source, location, disposition, movement, rights with respect to or ownership of that property;
c) acquires, possesses, uses or otherwise deals with that property; or
d) participates in, associates with or conspires to commit, attempts to commit, or aids and abets, or facilitates, counsels or procures the commission of any of the above acts.

2 '*Tipping off*' means informing a suspect or third party that a report of suspicion of money laundering has been made to the FIU or to the Money Laundering Compliance Officer (hereinafter "MLCO") or that the suspect is being investigated.

3 '*Misrepresentation*' occurs when a person knowingly makes a false, fictitious or fraudulent statement or representation, or makes, or provides, any false document, knowing the same to contain any false, fictitious or fraudulent statement or entry, to a reporting entity, or to a supervisory authority or to the Mauritius Financial Intelligence Unit (SFIU).

4 '*Malicious Reporting*' occurs when a person willfully gives any information to the Mauritius Financial Intelligence Unit (SFIU) or to an authorized officer, knowing such information to be false.

5. THE COMPANY'S ANTI MONEY LAUNDERING (AML) AND COUNTER-TERRORIST FINANCING (CTF) OBLIGATIONS

5.1. To maintain the company's integrity and reputation it is important to identify, report, and take precautions to guard against money laundering and financing of terrorism.

5.2. The nature of the Company's business requires it to abide by all of the above- mentioned anti-money laundering (AML) and countering the financing of terrorism (CFT) legislation and regulations.

A. In General

5.3. In order to prevent the Company's products and services from being used for the laundering of the proceeds of crime, it is required to establish appropriate and proportionate to the level of risk, systems and controls, and ensure their effective implementation, including, without limitation, the following:

a. Identifying our Clients;

b. Identifying, monitoring and reporting any kind of suspicious transactions;

c. Maintaining transaction records for a minimum of seven (7) years after the termination of our contractual relationships with our Clients;

d. Training our staff to recognize suspicious transactions and to fulfil all reporting obligations;

e. Depending on Client location, report any suspicious activities to authorities in several countries where the Company is offering its products and services.

B. Client Onboarding and Acceptance

5.4. In line with the foregoing, the Company has established the following rules for the 'onboarding and acceptance of Clients':

a. All Clients have to submit a valid 'Proof of Identity (POI)', which must be fully legible, colored with full name, surname and clear and identifiable photograph; any of the following may be submitted:

- Client's valid passport,
- Valid National Identification Card,
- Valid Driver's License.

b. All Clients have to submit a valid 'Proof of Residence (POR)'; POR must have been issued in the individual's name and must contain the individual's residential address; it cannot be older than three (3) months and cannot be the same as the document provided as proof of identity; any of the following may be submitted:

- utility bill (electricity or water authority bill, internet or phone services bill);
- bank statement (current, deposit or credit card account).

c. All Clients are screened against a 'Risk Screening Tool Database', in order to ensure that the identity of the Client in question does not match with any persons who are known to have criminal background or are subject to sanctions, or is associated with banned entities such as individual terrorists or terrorist organizations, etc. In addition, the Clients are screened against records of PEPs (including their close associates

and family members), which are also covered in the Risk Screening Tool database;

d. All Clients are classified into different risk categories in line with the provisions of the Client Classification section of the Company's AML Manual. The following risk factors, inter alia, are accounted for when considering the level of risk involved with each Client relationship:

- cumulative amount of funds deposited into the Client account/accounts;
- country of residence;
- nationality;
- results of risk screening, etc.

e. Depending on the level of risk assigned to the Client, additional checks may be required for Clients, falling within higher risk categories; enhanced due diligence is conducted for such Clients, whereby the source of funds and/or source of wealth, and any other information deemed necessary, are verified additionally to the checks conducted within the standard due diligence.

f. Following the necessary checks, and based on the perceived level of risk, associated with each Client relationship, the decision is made to either proceed with a Client's application or reject it. For all the Clients classified as high-risk, an approval from either the Company's 'Money Laundering Compliance Officer (MLCO)', 'Compliance Officer (CO)' or 'Chief executive Officer (CEO)' is required;

g. 'Politically Exposed Persons (PEPs)'[5], their family members and close associates are classified as higher risk and must undergo enhanced due diligence procedures.

5 The FATF's latest definition of 'Politically Exposed Persons (PEP)' includes the following:

- *Foreign PEPs*: individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of state or Heads of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- *Domestic PEPs*: individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, members of parliament, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- *PEPs by function*: Persons who are or have been entrusted with a prominent function by a state-owned enterprise or an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

5.5. The screening of all Clients against the applicable UN, US and EU sanctions lists, is an integral part of the screening of Clients against the Company's 'Risk Screening Tool Database'; where a Client is identified as a true match on any of the above sanctions list during the risk screening process, the

account opening application of the Client in question shall be rejected and no business activity shall be initiated with such Client.

5.6. In line with the foregoing, the following are not accepted by the Company as Clients (the list below is not exhaustive):

a. where sufficient KYC information could not be obtained/confirmed or as per the Client's risk categorization;

b. the Client matches the person in the sanction lists during risk screening and the match is confirmed to be a true match by the designated Compliance Officer (CO) or the Money Laundering Compliance Officer (MLCO);

c. the Client matches the person in the lists with criminal records during risk screening and the match is confirmed to be a true match by the designated Compliance Officer (CO) or the Money Laundering Compliance Officer (MLCO);

d. Clients from countries on the list of non-cooperatives jurisdictions with the FATF;

e. Clients from restricted jurisdictions, as per the list published on the Company's Website(s);

f. Clients whose accounts are in name of companies, the shares of which are in bearer form;

g. Clients whose accounts are in the name of a Trust.

C. Ongoing Client Monitoring

5.7. The ongoing monitoring of Client relationships is comprised of two sets of measures:

a. All Client records are kept up-to date, KYC information and documents are updated regularly; these updates include, for instance, ongoing risk screening for all existing Clients against the Company's 'Risk Screening Tool Database'; such Client information updates may result in re-classification of the Client into a different risk category, in which instance, the rules for ongoing monitoring over this Client relationship will be reset to align with the updated risk category;

b. Ongoing screening of existing Clients against the Company's 'Risk Screening Tool Database' includes screening against the applicable UN, US and EU sanctions lists; in the event that a Client is identified as a true match on any of the above sanctions lists during the ongoing risk screening process, the account of the Client shall be closed, and no further business activity shall be conducted with such Client;

c. The Company's transaction monitoring rules are designed in accordance with the applicable risk classification of a Client relationship; ongoing monitoring of each Client's activity is conducted

by the Company's Compliance Officers and Money Laundering Compliance Officers, in "real-time" and retrospectively.

D. Internal and External Reporting

5.8. 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 Mauritius; (b) the country of origin of any funds transmitted to the Company; and (c) the destination country of any funds refunded by or withdrawn from the Company.

5.9. The Company reserves the right to refuse the processing of a transfer of funds at any stage if it believes it to be connected in any way to criminal activities or money laundering.

5.10. The Company is obliged to report all suspicious transactions and is prohibited from informing Clients in case they have been reported for suspicious account activity.

5.11. As indicated above, any such misuse of an account held with the Company for money laundering, terrorist financing and/or related offences that is reported to the relevant authorities may result in criminal prosecution.

6. POLICY REVIEW AND UPDATE

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

6.2. Should you have a question about our Money Laundering Prevention Policy please direct your questions to our Support Department: contact@multifi.trade