PFH MARKETS LIMITED

("the Company")

www.pfhmarkets.com

("Brand Name")

Anti–Money Laundering Policy & Combating Terrorist Financing

TABLE OF CONTENTS

1. PREAMBLE

The policy is formulated in accordance with the provisions of the Financial Intelligence Authority Anti–Money Laundering and Combatting the Financing of Terrorism Handbook 2020 (FIA AML-CFT Handbook 2020) (updated on 9th March 2023) to help the Company assess the adequacy of its internal systems and controls and remedy deficiencies with the aim of combatting laundering of criminal proceeds, the financing of terrorism and the financing of proliferation of weapons of mass destruction.

The FIA encourages all reporting institutions to apply appropriate customer due diligence or enhanced customer due diligence measures when dealing with customers or handling transaction connected with any of the jurisdictions that have been identified by the FATF.

Financial Action Task Force 40 Recommendations intended to ensure that reporting institutions understands and comply with the requirements and obligations imposed on them. Besides bringing the recommendation up to date in addressing new and emerging threats, the 2012 revision of the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF 40 Recommendations), sought to clarify and strengthen many of its existing obligations as well as to reduce duplication of the Recommendations. One of the new Recommendations introduced is on the obligation of countries to adopt a risk–based approach in identifying, assessing, and understanding the countries' ML/TF risks, which places further expectation to assess and mitigate ML/TF risks.

2. Definition of Money Laundering

Chapter 2.1 of the FIA AML and CFT Handbook 2023 has defined "money laundering" as the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities and turning them into legitimate funds.

The Palermo Convention also defines money laundering as:

- The conversion or transfer of property, knowing it is derived from a criminal offense for the purpose of concealing its illicit origin or of assisting any person who is involved in the commission of crime to evade the legal consequences of his / her actions.
- The concealment of disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property knowing that it is derived from a criminal offense.
- The acquisition, possession or use of property, knowing at the time of receipt that it was derived from a criminal offense of from participation in a crime.

Several jurisdictions also use the legal principle of "willful blindness" in money laundering cases to prove knowledge. Willful blindness means the deliberate avoidance of knowledge of the facts or purposeful indifference and have held that willful blindness is the equivalent of actual knowledge of the illegal source of funds or of the intentions of a customer in a money laundering transaction.

2.1 Traditional Money Laundering Cycle:

The process of money laundering involves creating a web of financial transactions to hide the origin and the true nature of these funds.

The process of Money Laundering regardless of its degree of complexity, is accomplished in three stages, namely, (a) the Placement Stage, (b) Layering Stage, and (c) Integration Stage.

a. **Placement:** Physical disposal of criminal proceeds (large amount of cash) and initial introduction of illicit funds into a financial services institution.
Examples:
- Foreign Exchange – Purchasing of foreign currencies with illegal funds
- Currency smuggling – Cross-border physical movement of cash or monetary

b. **Layering:** Movement of funds (e.g., through multiple transactions) from institution to institution to obfuscate the source and ownership of funds and to separate the criminal proceeds from their source by the creation of complex layers of financial transactions designed to disguise the audit trail and provide the appearance of legitimacy.
Examples:
- Electronically moving funds from one country to another and dividing then into advanced financial options and or markets.
- Moving funds from one financial institution to another or within accounts at the same institution.
- Converting the cash placed into monetary instruments.
- Investing in real estate and other legitimate business.
- Placing money in stocks, bonds, or life insurance products.
- Using shell companies to obscure the ultimate beneficial owner and assets

c. **Integration:** The placing of laundered proceeds back into the economy in such a way that they re-enter the market appearing as normal and legitimate funds.
In the integration stage, it is very difficult to distinguish between legal and illegal wealth.
Examples:
- Purchasing luxury assets like property, artwork, jewelry, or high-end automobiles.
- Investment in commercial/industrial
- Financial investments

3. What is Financing of Terrorism?

The FIA AML-CFT handbook defines terrorist financing (TF) as the financial support, in any form, of terrorism or those who encourage, plan, or engage in terrorism. TF differs from ML in terms of the source of funds as it can either be legitimate or illegitimate.

Traditional Terrorist Financing Cycle

a. Collection: Funds are often acquired through seeking donations, use of charities or nonprofit organizations.
b. Transmission: Where funds are pooled and transferred to a terrorist.
c. Use: Where the funds are used to finance terrorist acts, training, propaganda, etc.

4. The consequences of money laundering and terrorist financing

Money laundering and terrorism financing (ML/TF) continues to be an on-going threat which has the potential to adversely affect the country's reputation and investment climate which may lead to economic and social consequences.

- reputational damage from being perceived as being a haven for money launderers and terrorist financiers, leading to legitimate business taking their business elsewhere;
- attracting criminals including terrorists and their financiers to move to or establish new business relationships within the jurisdiction;
- damaging the legitimate private sector who may be unable to compete against front companies; weakening of financial institutions which may come to rely on the proceeds of crime for managing their assets, liabilities and operations, plus additional costs of investigations, seizures, fines, lawsuits, etc;
- economic distortion and instability; or
- increased social costs to deal with additional criminality such as policing costs or hospital costs for treating drug addicts.

5. Scope

This policy is for PFH MARKETS LIMITED (www.pfhmarkets.com.) directors, officers and staff handling the financial services in conjunction with the AML and CFT Handbook 2020.

6. Implementation of Anti Money Laundering Policy

The primary goal of an AML/CFT policy is to protect the Company against money laundering, terrorist financing and other financial crimes and to ensure that the Company is in full compliance with relevant laws and regulations.
As per Regulations 22 of FIAMLA 2018, every reporting person shall implement programmes against money laundering, hence PFH MARKETS LIMITED shall:

a. appoint a resident Compliance officer and ground Compliance Manager, resident MLRO and DMLRO (Compliance team) responsible for the implementation and ongoing compliance with the Saint Lucia FIA Anti Money Laundering Guidelines. The Compliance team will define/implement appropriate criterion for identifying the suspicious transactions and reporting of the same to Saint Lucia Financial Intelligence Unit.
b. ensure that high standards screening is in place when hiring employees.

c. provide ongoing training programme for all the Company's employees including directors and officers to educating them on the AML/CFT laws and regulations in order for them to identify transactions which may be linked to money laundering of terrorism financing.
d. an independent audit function to review and verify compliance whether the measures taken are effective and in accordance with the Act and the above-mentioned Regulations.

The relevant employees such as on-boarding team, sales team, compliance, etc. in the Company should conduct customer due diligence when they:

a. Establish business relations.
b. Carry out an occasional transaction or a wire transfer above the specified threshold.
c. Have a suspicion of money laundering or terrorist financing.
d. Have doubts about the veracity or adequacy of previous obtained client's identification information.

In compliance with the FIA AML-CFT handbook, CDD measures that should be undertaken by the Firm under the relevant legislation include:

a. identifying and verifying the identity of each client;
b. identifying and verifying the identity of the ultimate beneficial owner and taking risk-based and adequate measures to understand the ownership and control structure of the clients;
c. obtaining information on the purpose and intended nature of the business relationship (the inability of the Onboarding/compliance team to understand the rationale for business relationship may result to identify potential money laundering and financing of terrorism activity;
d. undertaking ongoing due diligence and monitoring on the business relationship and scrutiny to ensure that the transactions being conducted by the clients are consistent with the Firm's knowledge of the customer and its business and risk profile, including the source of funds and wealth; and
e. achieving each of the above measures by using reliable, independent sourced document, data or information and ensuring that the documents, data or information collected under the CDD process are kept up-to-date.

Please refer to the CDD manual for the detailed identification and verification of clients documents.

7. The Risk-Based Approach

In applying CDD measures as listed above, the Firm will follow a risk-based approach which aim is to support the development of precautionary and mitigating measures that are in line with of ML and TF risks identified by the Firm in the most cost-effective and proportionate way when transacting with clients and determining their associated risk profile.

A risk-based approach starts with the identification and assessment of the risk that must be

managed. In Accordance with the FIA AML-CFT handbook, the following diagram sets out the basic risk assessment process:

7.1 Business Risk Assessments

Section 17(2) of the FIAMLA requires businesses to assess 6 keys areas when undertaking the business risk assessment amongst other risk factors:

a. the nature, scale and complexity of the financial institution's activities;
b. the products and services provided by the financial institution's;
c. the persons to whom and the manner in which the products and services are provided;
d. the nature, scale, complexity and location of the customer's activities;
e. reliance on third parties for elements of the customer due diligence process; and
f. technological developments.

The assessment should consider the operational risks, reputational risks and legal risks posed by the new technologies and appropriate action should be taken to mitigate the risks that have been identified.

Operational Risks

Operational risk arises due to the deficiencies in system reliability or integrity, staff who does not fully understand the new technology or though channels of distributing software updates.

Reputational **Risks**

Reputational risk may arise when systems or products failed and cause negative clients reaction. If the affected systems were used to collect and maintain clients information, this may lead to serious reputational concerns.

Legal Risks

Legal risks arise due to non-compliance with the key regulations such as the FIAMLA and FIAML Regulations 2018.

Compliance Risk
Risk of loss due to failure of compliance with key regulations governing the Capital Markets Registry activities.

The above risk factors are non-exhaustive list, and the Company will assess and eventually decide the risk elements to be considered in order to demonstrate an effective and robust business risk assessments.

7.2 Client Risk Assessments

Prior to establishment of a business relationship, a client risk assessment identifying the risk of ML/TF must be undertaken such as obtaining documents and information from the client, verification of such documents and ongoing monitoring of the business relationship.

The FIA has no objection to the Firm having higher risk clients, if they have been adequately risk assessed and EDD must be obtained.

For higher risk customers, FATF also recommends obtaining the approval of senior management to commence or continue the business relationship.

8. Monitoring of Transactions and Activity

As per the chapter 9 of the FIA AML/CFT handbook, it is requirement for the Firm to ensure the regular monitoring of any transactions and other activity carried out as part of the business relationship; it is one of the most essential aspects of effective ongoing client due diligence measures. It is important that the Firm understand the client's background and is aware of any UBO changes throughout the business relationship.

The Firm can usually only determine when there is a reasonable ground for suspecting that ML-TF is occurring when a transactions and activity falls outside the normal expectations for a particular business relationship.

In accordance with Regulation 3(1) (e) of the FIAML Regulations 2018, financial institutions should conduct ongoing monitoring of a business relationship, including:

i. Scrutiny of transactions undertaken throughout the course of the business relationship including the source of funds, to ensure that the transactions are consistent with the Firm knowledge of its clients business and risk profile;
ii. Ensure that the documents or data collected are kept up to date by undertaking review of existing records.

Enhanced due diligence should be applied for clients or UBO who becomes a PEP during the course of the business relationship and the Firm should seek the senior management approval whether or not to continue the business relationship.

When conducting ongoing monitoring, below are examples of red flags which may indicate high risk transactions or activity:

(a) an unusual transaction in the context of the financial institution's understanding of the business relationship (for example, abnormal size or frequency for that customer or peer group,

or a transaction or activity involving an unknown third party);

(b) funds originating from, or destined for, an unusual location, whether specific to an individual business relationship, or for a generic customer or product type;

(c) transactions or activity unexpectedly occurring after a period of dormancy;

(d) unusual patterns of transactions or activity which have no apparent economic or lawful purpose;

(e) an instruction to effect payments for advisory or consulting activities with no apparent connection to the known activities of the customer or their business;

(f) the involvement of charitable or political donations or sponsorship; or

(g) a relevant connection with a country or territory that has significant levels of corruption, or provides funding or support for terrorist activities.

The Firm must remain conscious that under the FIAMLA, they have an obligation to prevent and detect ML and TF.

9. Reporting Suspicious Transaction

The Compliance/MLRO is responsible for channeling all internal suspicious transaction reports received from the employees. Upon receiving any internal suspicious transaction, the Compliance/MLRO must evaluate the grounds of suspicion, once it is confirmed, the Compliance/MLRO must submit the STR. In case, there is no reasonable grounds, Compliance/ MLRO must document and file the decision, supported by relevant documents.

The Compliance/MLRO must submit the completed suspicious transaction report form in the through the following modes:

By Registered post or hand delivery to:

Financial Intelligence Authority
P.O.Box GM959
Gablewoods North P.O.
Castries LC02 501
Saint Lucia

The Compliance/MLRO must ensure the suspicious transaction report is submitted within the next working day; from the date the Compliance/MLRO establishes the suspicion.

The compliance/MLRO must ensure that the suspicious transaction reporting mechanism is operated in secured environment to maintain confidentiality and preserve secrecy.

10. Maintenance of Records

PFH MARKETS LIMITED must establish a mechanism to keep the relevant records including any account, files and business correspondence and documents relating to transactions, those obtained during the CDD process.

The Compliance Manager shall ensure that the records related to Suspicious Transaction are preserved and maintained, for a period of seven (7) years and must include the following information:

a. nature of the transactions;
b. amount of the transactions;
c. date on which the transaction was conducted;
d. parties to the transaction;
e. all suspicious transactions, whether or not made in cash.

11. Retention of records

The records are required to be kept including the corresponding/relevant records must be maintained for a period of seven (7) years.

Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards including driving license, or any other government issued identity cards), account files and business correspondence should also be kept for the same period.

In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case is closed/decided/adjudicated.

12. Review of the Policy

The Compliance Manager along with the senior management responsible for over – all monitoring of the level of compliance activities by PFH MARKETS LIMITED shall review this policy as and when any changes take place either in the AML-CFT Handbook and/ or the regulations issued by the Financial Intelligence Authority of Saint Lucia.

13. Training

The Compliance Manager shall ensure that adequate training is imparted to all the concerned Officers handling the activities of the company so as to ensure that the contents of the guidelines are understood and to develop awareness and vigilance to guard against money laundering and terrorist financing.

14. Sanctions List

A sanction list checks needs to be completed for every Client, regardless of the type of entity. The Compliance Manager must check against the FATF list and where applicable against the United States Treasury's Office of Foreign Assets Control (OFAC); as well as the United Sanctions List.

OFAC: https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

UN: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

If you have any questions about this policy document, please address all correspondence: For the attention of
PFH MARKETS LIMITED
Compliance Department
Email: compliance@pfhmarkets.com