Prime FX CFD Ltd

(“Prime”)

KNOW YOUR CUSTOMER, ANTI MONEY LAUNDERING AND COMBATTING TERRORISM FINANCING POLICIES AND PROCEDURES MANUAL

Contents

1. Introduction

Prime FX CFD Ltd ("**Prime**") is a financial services company, having its registered office at 1st Floor, The Sotheby Building, Rodney Village, Rodney Bay, St Lucia. Registered Company Number 2023 – 00443.

As a responsible financial company, Prime comply with the anti-money laundering laws in force along with the various guidelines and regulations related with global Financial Intelligence Units and other international standards. This Anti-Money Laundering and Combatting Terrorism Financing Policies and Procedures Manual (the "**Manual**") displays the procedures applicable to the Company and which must be adhered to by all staff members and officers working in the Company.

Staff members and officers should understand the procedures set out herein and the Company's policies with regards to Customer Due Diligence.

All the procedures set in this Manual, on the Prevention of Money Laundering and Terrorist Financing, the Anti-Money Laundering and Countering the Financing of Terrorism Handbook should be adhered to at all times. Failure to do is a breach of your duty towards the Company and the regulatory authorities. This Manual shall be read in conjunction with standard AML/CFT Codes, the AML/CFT Handbook, the Financial Intelligence Anti-Money Laundering Act 2002, and the Financial Intelligence Anti-Money Laundering Regulations 2018.

2. List of Officers

Money Laundering Reporting Officer:	Mr. Des Grech
Compliance Officer:	Mr. Des Grech

3. Definitions

AML/CFT	Anti-money laundering and combatting the financing of terrorism and proliferation
Applicant for Business	A person who seeks to establish a business relationship, or carries out an occasional transaction, with a reporting person
CDD	Customer Due Diligence
Company	Prime FX CFD Ltd or any registered trading name under Prime FX CFD Ltd
FATF	Financial Action Task Force
FIAMLA	Financial Intelligence and AML Act 2002 as amended from time to time
FIAMLR	Financial Intelligence and Anti Money Laundering Regulations 2018 as amended from time to time
FIU	Financial Intelligence Unit
AML/CFT Code	Code on the Prevention of Money Laundering & Terrorist Financing
AML/CFT Handbook	The Anti-Money Laundering and Countering the Financing of Terrorism Handbook as may be amended from time to time.
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
NCCT	Non-Cooperative Countries and Territories
Proliferation	(a) the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, import, export, transshipment, or use of: (i) nuclear weapons (ii) chemical weapons (iii) biological weapons (iv) such other materials, as may be prescribed, which are related to nuclear weapons, chemical weapons or biological weapons; or (b) the provision of technical training, advice, service, brokering or assistance related to any of the activities specified in paragraph (a)
Reporting Person	Bank, financial institution, cash dealer or member of a relevant profession or occupation
STR	Suspicious Transaction Report Form prescribed by the FIAMLA

4. Money Laundering & Terrorist Financing Definitions

4.1. Money Laundering

The definition of money laundering is given in Section 3 of the Financial Intelligence and Anti-Money Laundering Act which provides that:

> *Any person who –*
>
> *(a) engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or*
> *(b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into St Lucia any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime, where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime,*
>
> shall commit an offence.

The AML/CFT Code provides that money laundering is any process that conceals the origin or derivation of the proceeds of crime so that the proceeds appear to be derived from legitimate source.

It should be noted that money laundering is not only associated with organized crime or drug trafficking but also occurs when a person deals with another person's direct or indirect benefit from criminal activities.

Money laundering can, in summary, be defined to be a three-stage process, as follows:

a. Placement Stage – where illegal money or property is introduced into the financial system
b. Layering Stage – where property undergoes a series of transactions, concealing its origin and making it appear to be legitimate; and
c. Integration Stage – the stage where laundered money enters within the legitimate economy.

The Company's services can be misused in these stages. Stages (b) and (c) above in the money laundering process are where the Company will be most vulnerable. The Company's vulnerability should therefore be fully measured and understood.

4.2. Terrorist Financing

The AML/CFT Code states that *'All acts of terror and the terrorist groups that commit them require funding in much the same way that criminal organizations require money to further their criminal activities. Since the dreadful events of September 11th in the United States, the prevention of the financing of terrorism by the financial sector has gained equal status with the prevention of the laundering of the proceeds of crime.'*

The definitions of money laundering and terrorist financing have differences and similarities as well. To start with, the differences are:

(a) Terrorist financing is an activity in support of future illegal acts, whereas money laundering generally occurs after the commission of illegal acts; and
(b) Legitimate property is often used to support terrorism and the origin of laundered money is illegitimate.

Similarities include:

(a) Terrorist groups are often involved in other forms of criminal activities which may in turn fund their terrorist activities
(b) Both money launderers and terrorist financiers require the assistance of the financial sector to further their aims and acts.

5. Customer Due Diligence Procedures ("CDD")

In order to detect and prevent money laundering and financing of terrorism it is fundamental that the Company knows and understands its customers / clients.

Prior to establishing a business relationship with an Applicant for Business, as well as on an ongoing basis, the Company shall use a risk-based approach to determine the necessary CDD measures that should be applied.

The CDD measures include:

- Identification and verification of the identity of the Applicant for Business and principals
- Determining the purpose and nature of the business relationship
- Conducting ongoing due diligence and monitoring on the business relationship and business activities, and verification of the transactions throughout the business relationship

5.1. Identification and verification of applicant for business who are natural persons

It is fundamental for the Company to identify and verify the identity of all its clients and other business partners.

5.1.1. Primary Verification

It is imperative that identification documentation is obtained and verified.

Identity documentation must be obtained and retained to verify the information provided by the clients on their identity. The documentation must be pre-signed and must be either in an original form or must be certified appropriately and should bear a photograph of the principal.

The following primary documentation are acceptable for the verification of the identity of a natural person:

1. Current valid passports
2. National Identity cards
3. Current valid driving licenses

In addition to the primary identity documentation, we must obtain additional verification of identity, that is, secondary identity documentation. The secondary documentation must be, as for primary identity verification, either in an original form or must be appropriately certified. The following documentation are acceptable for the verification of the address of a natural person:

1. A recent utility bill (less than 6 months old); or
2. A recent bank or credit card statement dated (less than 6 months old)

5.2. Identification and verification of Applicant for Business who are legal persons

Legal persons include bodies corporate, partnership, foundation, associations, or any other body of persons other than legal arrangements.

In the case of a legal person Applicant for Business include:

a. Directors
b. Shareholders
c. Promoters
d. Beneficial Owners and ultimate beneficial owners
e. Controllers
f. Officers
g. Bank mandate
h. Power of Attorney holders, etc.

5.3. Identification and verification of applicant for business who are Legal Arrangements

Trusts do not have separate legal personality and therefore form business relationships through their business.

Where the Applicant for Business is a legal arrangement is it essential to:

- Understand the ownership and control structure of the applicant for business
- Verify and establish the existence of the legal arrangement
- Determine the identity of the principals of the legal arrangement

In case of legal arrangement, principals of Applicant for Business include:

a. Settlors or Contributors of capital
b. Trustees
c. Beneficiaries
d. Protectors
e. Enforcers

5.4. Declaration of Source of Funds / Property / Source of Wealth

It is a requirement to verify the origin of the source of funds and source of wealth both at the outset of a client relationship and on an ongoing basis throughout the duration of the business relationship.

A risk-based approach should be used to establish the source of funds of each client. In some cases, it may also be considered to obtain information on the client's source of wealth.

All funds transferred should be known and should fall within the business objectives and risk profile of each client.

Source of funds is the activity of transaction which generate the funds for the client, whereas source of wealth refers to the activities which have generated the total net worth of the client.

If CDD documentation is unsatisfactory, we should ask for additional documents or disengage from relationship and or inform the MLRO.

6. High and Low Risk Clients

6.1. CDD and Risk Profiling

CDD extends beyond the identification and verification of the client. It also includes the identification of risks associated with the client, his transactions, and the business activities. It is therefore essential to conduct an identification of the potential risks of a business relationship, i.e., risk profiling. Once the risk has been identified, adequate measures must be implemented to mitigate these risks. Such risks would include:

a. Criminal risk of money laundering
b. Reputational risk
c. Legal risk
d. Credit risk
e. Fiduciary risk
f. Regulatory risk; and
g. Operational risk amongst others

Various factors must be taken into consideration to assess the risks to which a business relationship may expose us to and to accordingly evaluate the clients. These factors include the following:

a. Identity and occupation of client
b. Nature and type of client
c. Business activities

d. Commercial purpose of the relationship
e. Location of the client's residence
f. Geographical location of the client's business interests and/or assets
g. Value and nature of the assets involved
h. Source of funds, and source of wealth
i. Delegation of authorities or powers

All the above factors need to be properly considered so that risks are mitigated. A risk assessment should be conducted for each client prior to engaging into any relationship with the client.

6.2. Low Risk Relationship and Simplified or Reduced Due Diligence

Where the risk level is low and where information on the identity of the applicant for business is public information or where adequate checks and controls exist elsewhere, we may apply reduced or simplified due diligence measures when identifying and verifying the entity of the applicant for business.

6.3. High Risk Relationship and Enhanced CDD measures

Enhanced CDD measures should be applied in all high-risk business relationships, customers and transactions and where the risk if money laundering or terrorist financing is identified. This entails taking additional steps in relation to identification and verification.

Enhanced CDD must be conducted in the following circumstances:

a. Politically Exposed Person (PEP)

As per the FIAMLR PEP means a foreign, domestic or international PEP. The FIAMLR further provides a definition for each type of the hereinabove identified PEP.

Domestic PEPs means' a natural person who is or has been entrusted domestically with prominent public functions in St Lucia and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state- owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

Foreign PEPs means' a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

International organisation PEP means a person who is or has been entrusted with a prominent function by an international organisation and includes members of senior management or individuals who have been entrusted with equivalent functions, including directors, deputy directors and members of the board or equivalent functions and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

Enhanced due diligence must be applied at all times when dealing with PEPs.

b. Non- face to face business relationship and non-cooperative countries and territories ("NCCT") and non-equivalent jurisdictions

Enhanced due diligence must be applied when dealing with non-face-to-face clients and business relationships involving countries which are non-cooperative jurisdictions, or which have been the subject of FATF Public Statements for deficiencies in their AML/CFT systems.

The above does not constitute an exhaustive list of the situations in which enhanced due diligence must be applied. The Company is required to undertake a risk assessment of all its clients, and other relevant parties using a risk-based approach and accordingly determine the appropriate risk framework and due diligence process and procedure.

7. On-Going Transaction Monitoring and Reporting Duties

It is essential that the business relationship is monitored on an ongoing basis to ensure that it is consistent with the nature of business stated at the establishment of the relationship and so as to detect and prevent any potential money laundering or terrorist financing.

As part of the ongoing monitoring, periodic reviews using a risk-based approach of the existing records should be conducted. It must also be ensured that up to date information and KYC documents are obtained.

7.1. Suspicious Transactions

The definition of suspicion transaction is provided in the FIAMLA as "*…. a transaction which* –

(a) gives rise to a reasonable suspicion that it may involve

(i) the laundering of money or the proceeds of any crime; or

(ii) funds linked or related to, or to be used for, the financing of terrorism or proliferation financing, or any other activities or transaction related to terrorism as specified in the Prevention of Terrorism Act or under any other enactment, whether or not the funds represent the proceeds of a crime

(b) is made in circumstances of unusual or unjustified complexity

(c) appears to have no economic justification or lawful objective

(d) is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or

(e) gives rise to suspicion for any other reason".

FIAMLA further defines transaction as follows: -

"*Transaction includes:*

(a) opening an account, issuing a passbook, renting a safe deposit box, entering into a fiduciary relationship or establishing any other business relationship, whether electronically or otherwise; and

(b) a proposed transaction or an attempted transaction."

Potential money laundering activity often occurs in the form of unusual of unexpected patterns.

Having recognized that a transaction is suspicious, you should report it internally in writing to the MLRO in the format below:

7.2. Disclosure Form ("Disclosure Form"):

Name and contact details of the entity	
Contact Details of Introducer / Agent	
Countries and Territories Involved	
Other related entities	
Date and Summary of transactions	
Description of suspicious activity	
Reason for Suspicion	
Name and capacity of the Person making the disclosure	
Signed and dated	

7.3. Red flags to look for or consider in order to recognize a suspicious transaction

A non-exhaustive conclusive list of red flags is set below:

- Complex transactions
- Unusually large transactions
- Transaction conducted in an unusual pattern
  Transaction that does not appear to have an apparent economic or lawful purpose
- Any relationship or arrangement which that appears not to have a commercial justification
- A transaction which is out of the normal business pattern of the Company
- Fund transfers to and from FATF NCCTs or countries that are known to be involved with drug trafficking or terrorism
- Fund transfers to and from PEPs without justification
- Large transaction settled in by cash or bearer instruments
- The client's reluctance to provide documentation asked for
- Activities are inconsistent with CDD information held
- Any activity that casts doubt over the true identity of a client or its principals

If any one or more of the above flags is present, it should be reported to the MLRO by using the Disclosure Form. Upon receipt of the Disclosure Form the MLRO will investigate and decide on the next course of action.

ANNEX 1

VERSION	LAST REVIEW DATE	REVIEWED BY
1.1	01 September 2023 (date created)	D Grech