NobleFXM

Anti-Money Laundering

Effective Date: [TO BE CONFIRMED]
Version: DRAFT v1
Classification: Confidential

THIS DOCUMENT IS A DRAFT FOR QUALIFIED LEGAL COUNSEL REVIEW.
IT DOES NOT CONSTITUTE FINAL LEGAL ADVICE AND IS NOT INTENDED FOR CLIENT DISTRIBUTION.

NobleFXM, Ltd
Saint Lucia International Business Company (IBC)
Registration No. 2026-00159
Ground Floor, The Sotheby Building, Rodney Bay, Gros-Islet, Saint Lucia

ANTI-MONEY LAUNDERING

Effective Date: [TO BE CONFIRMED]

1. INTRODUCTION AND PURPOSE

NobleFXM, Ltd ("the Company"), a Saint Lucia International Business Company (IBC) with registration number 2026-00159, is committed to the prevention of money laundering, terrorist financing, and other forms of financial crime. This Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") Policy sets out the Company's framework for detecting, preventing, and reporting suspicious activities in compliance with applicable laws and regulations.

This Policy applies to all directors, officers, employees, contractors, and agents of the Company (collectively, "Personnel"), as well as to all business relationships and transactions conducted through the Company's trading platforms and services.

[COUNSEL TO REVIEW: Confirm that this Policy satisfies the requirements of the Saint Lucia Money Laundering (Prevention) Act (Cap. 12.20), the Proceeds of Crime Act (Cap. 3.04), the Counter-Terrorism Act, the Suppression of the Financing of Terrorism Act, and any regulations or guidelines issued by the Financial Intelligence Authority (FIA) of Saint Lucia. Confirm alignment with FATF Recommendations as adopted by CFATF.]

2. REGULATORY FRAMEWORK

The Company's AML/CFT programme is designed to comply with, at a minimum:

- The Money Laundering (Prevention) Act of Saint Lucia (Cap. 12.20), as amended
- The Proceeds of Crime Act of Saint Lucia (Cap. 3.04)
- The Suppression of the Financing of Terrorism Act of Saint Lucia
- The Counter-Terrorism Act of Saint Lucia
- Guidelines and directives issued by the Financial Intelligence Authority (FIA) of Saint Lucia
- Applicable United Nations Security Council Resolutions regarding sanctions
- Caribbean Financial Action Task Force (CFATF) Recommendations
- Financial Action Task Force (FATF) Recommendations, as adopted regionally

[COUNSEL TO REVIEW: Verify the completeness of the above statutory references and confirm whether additional Saint Lucia or regional legislation applies to IBC-registered financial services entities.]

3. COMPLIANCE OFFICER

The Company shall appoint a designated Money Laundering Reporting Officer ("MLRO") who shall be responsible for:

- Overseeing the implementation and effectiveness of this Policy
- Receiving, reviewing, and investigating internal suspicious activity reports
- Filing Suspicious Transaction Reports ("STRs") with the Financial Intelligence Authority (FIA) of Saint Lucia
- Maintaining AML/CFT records and documentation
- Coordinating with law enforcement and regulatory authorities
- Ensuring ongoing staff training and awareness
- Reporting to the Board of Directors on AML/CFT matters

The MLRO shall have sufficient authority, independence, and resources to discharge their responsibilities effectively. The identity of the MLRO shall be communicated to all Personnel and to the FIA.

Contact for compliance matters: compliance@noblefxm.com

4. CUSTOMER DUE DILIGENCE (CDD)

The Company shall conduct Customer Due Diligence ("CDD") on all clients prior to establishing a business relationship and on an ongoing basis throughout the relationship. CDD measures include:

4.1 Standard CDD

ANTI-MONEY LAUNDERING

Effective Date: [TO BE CONFIRMED]

For all clients, the Company shall:

- Verify the identity of the client using reliable, independent source documents (government-issued photo identification, e.g., passport, national identity card, or driver's licence)
- Verify the client's residential address using proof of address documents (e.g., utility bill, bank statement, government correspondence) dated within the last three (3) months
- Obtain and verify the client's date of birth, nationality, and contact information
- Determine the purpose and intended nature of the business relationship
- Identify the source of funds and source of wealth where appropriate
- Screen the client against applicable sanctions lists, PEP databases, and adverse media sources
- Conduct liveness verification or selfie matching against the submitted identity document

4.2 Simplified Due Diligence (SDD)

Where the risk of money laundering or terrorist financing is assessed as low, the Company may apply simplified due diligence measures, provided that:

- The client falls within a category assessed as presenting a low risk
- The Company has documented its risk assessment justifying the application of SDD
- Ongoing monitoring of the relationship is maintained

[COUNSEL TO REVIEW: Confirm whether SDD is permissible under Saint Lucia law for IBC-registered entities providing leveraged trading services.]

4.3 Enhanced Due Diligence (EDD)

The Company shall apply Enhanced Due Diligence measures where a higher risk of money laundering or terrorist financing is identified, including but not limited to:

- Clients who are Politically Exposed Persons (PEPs), their family members, or close associates
- Clients from high-risk jurisdictions as identified by the FATF, CFATF, or the Company's own risk assessment
- Clients whose source of funds or source of wealth cannot be readily established
- Complex or unusually large transactions that have no apparent economic or lawful purpose
- Clients with adverse media coverage or law enforcement associations
- Non-face-to-face business relationships where additional verification may be required
- Correspondent banking or similar relationships

EDD measures may include: obtaining additional identification documents, requiring certified or notarised copies, obtaining a declaration of source of wealth, requesting bank references, conducting enhanced ongoing monitoring, and obtaining senior management approval for the business relationship.

5. POLITICALLY EXPOSED PERSONS (PEPs)

A Politically Exposed Person ("PEP") is an individual who is or has been entrusted with a prominent public function, including but not limited to heads of state, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned enterprises, and important political party officials.

The Company shall:

- Implement risk-based procedures to determine whether a client or beneficial owner is a PEP, a family member of a PEP, or a close associate of a PEP
- Obtain senior management approval before establishing or continuing a business relationship with a PEP
- Take reasonable measures to establish the source of wealth and source of funds
- Conduct enhanced ongoing monitoring of the business relationship
- Maintain PEP status determinations for the duration of the relationship and for the prescribed retention period after termination

[COUNSEL TO REVIEW: Confirm PEP definition scope under Saint Lucia legislation. Determine whether domestic PEPs require the same treatment as foreign PEPs.]

6. SANCTIONS SCREENING

The Company shall screen all clients, beneficial owners, and counterparties against applicable sanctions lists at the time of onboarding and on an ongoing basis. Applicable sanctions lists include, but are not limited to:

- United Nations Security Council Consolidated Sanctions List
- United States Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) List
- European Union Consolidated Sanctions List
- United Kingdom HM Treasury Sanctions List
- The First Schedule of the Terrorism (Suppression of Financing) Act of Saint Lucia
- ISIL (Da'esh) and Al-Qaida Sanctions List (UNSC Resolution 1267/1989/2253)
- Taliban 1988 Sanctions List (UNSC Resolution 1988)

The Company shall not establish or maintain business relationships with any individual or entity that appears on an applicable sanctions list. Any potential match shall be escalated to the MLRO immediately for review and determination.

The Company does not provide its services to individuals or entities from the Democratic People's Republic of Korea, Iran, South Sudan, Sudan, Yemen, or any country where such distribution or use would be contrary to local law or regulation.

7. SUSPICIOUS ACTIVITY MONITORING AND REPORTING

7.1 Ongoing Monitoring

The Company shall conduct ongoing monitoring of all client accounts and transactions to detect activity that is inconsistent with the Company's knowledge of the client, their business profile, risk profile, and source of funds. Monitoring measures include:

- Automated transaction monitoring systems to flag unusual patterns, including unusually large or frequent deposits/withdrawals, rapid movement of funds, and transactions inconsistent with the client's stated profile
- Manual review of flagged transactions by the compliance team
- Periodic review of client risk profiles and CDD information
- Monitoring for structuring (breaking large transactions into smaller amounts to avoid reporting thresholds)
- Monitoring for layering (complex series of transactions designed to obscure the origin of funds)

7.2 Suspicious Transaction Reporting

Where Personnel have knowledge, suspicion, or reasonable grounds to suspect that a transaction or attempted transaction involves proceeds of criminal activity, or is related to money laundering or terrorist financing, the matter shall be reported to the MLRO without delay.

The MLRO shall evaluate the internal report and, where warranted, file a Suspicious Transaction Report (STR) with the Financial Intelligence Authority (FIA) of Saint Lucia within the prescribed timeframe.

It is a criminal offence to "tip off" a client or any third party that a STR has been or is being filed, or that an investigation is being or may be conducted. All Personnel must exercise extreme caution to avoid tipping off.

[COUNSEL TO REVIEW: Confirm STR filing requirements, thresholds, and timelines under Saint Lucia law. Confirm whether the Company is also required to file Currency Transaction Reports (CTRs) above a certain threshold.]

8. RECORD KEEPING

The Company shall maintain records of all CDD documentation, transaction records, internal suspicious activity reports, STRs, correspondence with authorities, and training records for a minimum period of five (5) years after the

termination of the business relationship or the completion of the transaction, whichever is later.

Records shall be maintained in a manner that allows them to be made available to competent authorities in a timely fashion upon request.

[COUNSEL TO REVIEW: Confirm whether Saint Lucia law requires a longer retention period for any category of records. Confirm data protection obligations that may interact with retention requirements.]

9. EMPLOYEE TRAINING

All Personnel shall receive AML/CFT training upon joining the Company and at regular intervals thereafter (at least annually). Training shall cover:

- The Company's AML/CFT Policy and procedures
- Legal and regulatory obligations, including the consequences of non-compliance
- How to identify suspicious activities and transactions
- Reporting procedures for suspicious activities
- The prohibition on tipping off
- Updates to applicable laws, regulations, and typologies of money laundering and terrorist financing

Training records, including dates, content, and attendance, shall be maintained by the MLRO.

10. HIGH-RISK JURISDICTIONS

The Company maintains a list of high-risk jurisdictions based on assessments published by the FATF, CFATF, and its own internal risk assessment. Clients from high-risk jurisdictions are subject to Enhanced Due Diligence as described in Section 4.3.

The Company strictly prohibits the provision of services to individuals or entities from jurisdictions subject to comprehensive sanctions, including but not limited to: the Democratic People's Republic of Korea, Iran, South Sudan, Sudan, and Yemen.

The Company implements technical and operational measures to enforce its geographic restrictions. These include IP-based access controls, onboarding through third-party identity verification providers for KYC and, where applicable, biometric liveness checks, and policy-driven transaction monitoring. Accounts found to be in violation of the Company's geographic restrictions may be suspended or terminated in accordance with Company policy.

11. RISK ASSESSMENT

The Company shall conduct and document a comprehensive AML/CFT risk assessment on a periodic basis (at least annually) to identify, assess, and understand the money laundering and terrorist financing risks to which it is exposed. The risk assessment shall consider:

- Client risk factors (client type, geographic location, PEP status, industry)
- Product and service risk factors (complexity of products, delivery channels, new products)
- Geographic risk factors (jurisdictions of operation, client base geography)
- Transaction risk factors (volume, frequency, payment methods, cross-border transfers)
- Delivery channel risk factors (non-face-to-face onboarding, online-only relationships)

The findings of the risk assessment shall inform the Company's AML/CFT policies, procedures, and controls, and shall be reviewed and updated at least annually or when there is a material change in the Company's risk profile.

12. BENEFICIAL OWNERSHIP

Where the client is a legal entity, the Company shall take reasonable measures to:

- Identify the beneficial owner(s) of the entity — any natural person who ultimately owns or controls, directly or

indirectly, 25% or more of the shares, voting rights, or ownership interest, or who otherwise exercises effective control over the entity

- Verify the identity of the beneficial owner(s) using reliable, independent source documents
- Understand the ownership and control structure of the entity
- Obtain information on the purpose and intended nature of the business relationship

Where the beneficial owner(s) cannot be identified, the Company shall consider whether the business relationship should be established or continued and shall document the risk assessment accordingly.

13. THIRD-PARTY RELIANCE

The Company may rely on third-party service providers for elements of the CDD process, including identity verification and sanctions screening. Where the Company relies on a third party:

- The Company shall satisfy itself that the third party applies CDD measures and record-keeping requirements consistent with this Policy
- The Company shall obtain the necessary CDD information from the third party without delay
- The Company shall remain ultimately responsible for compliance with its CDD obligations
- The Company shall periodically review the adequacy and performance of the third-party provider

14. COOPERATION WITH AUTHORITIES

The Company shall cooperate fully with the Financial Intelligence Authority (FIA), law enforcement agencies, and other competent authorities in relation to AML/CFT matters. This includes responding to requests for information, providing access to records, and facilitating investigations.

Personnel shall not obstruct or interfere with any lawful investigation or inquiry by a competent authority.

15. POLICY REVIEW

This Policy shall be reviewed and updated at least annually, or more frequently as required by changes in applicable laws, regulations, guidance, or the Company's risk profile. Material amendments shall be approved by the Board of Directors.

Any questions regarding this Policy should be directed to the MLRO at compliance@noblefxm.com.