NobleFXM

KYC Verification Policy

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

KYC VERIFICATION POLICY

Effective Date: [TO BE CONFIRMED]

1. INTRODUCTION

NobleFXM, Ltd ("the Company"), a Saint Lucia International Business Company (IBC) with registration number 2026-00159, is committed to preventing the use of its services for money laundering, terrorist financing, fraud, and other financial crimes. As part of this commitment, the Company implements robust Know Your Customer ("KYC") procedures to verify the identity and suitability of all clients.

This KYC Verification Policy ("Policy") outlines the Company's requirements for client identification, verification, and ongoing due diligence. This Policy should be read in conjunction with the Company's Anti-Money Laundering Policy, Privacy Policy, and Agreement to Open an Account.

2. SCOPE

This Policy applies to all individuals and legal entities that apply to open a trading account with the Company. Customer Due Diligence is performed before a trading relationship is established (see the Anti-Money Laundering Policy, Section 4). Prior to satisfactory completion of verification, an applicant may be granted limited access to the Account as set out in Section 6 (Account Restrictions During Pending Verification), restricted to deposit functionality only. Trading features and withdrawals are enabled only once the Account is fully activated following satisfactory completion of verification.

3. IDENTITY VERIFICATION REQUIREMENTS

3.1 Individual Clients

All individual clients must provide the following documentation:

Proof of Identity (one of the following):

- Valid passport (must be current and not expired)
- National identity card (both sides, must be current and not expired)
- Government-issued driver's licence (both sides, must be current and not expired, accepted only if it contains a photograph and date of birth)

The identity document must:

- Clearly display the client's full legal name
- Include a clearly visible photograph of the client
- Display the date of birth
- Display the document's issue and expiry dates
- Be issued by a government authority
- Be in colour and fully legible (no cropped corners, no glare, no blurring)

Proof of Residential Address (one of the following, dated within the last three (3) months):

- Utility bill (electricity, gas, water, landline telephone — mobile phone bills are generally not accepted)
- Bank or credit card statement (from a recognised financial institution)
- Government-issued correspondence (e.g., tax notice, council/municipality letter)
- Tenancy agreement or mortgage statement (only if issued by a recognised institution)

The proof of address document must:

- Clearly display the client's full name matching the identity document
- Clearly display the full residential address (P.O. Box addresses are generally not accepted as a sole proof of address)
- Be dated within the last three (3) months
- Be in colour and fully legible

KYC VERIFICATION POLICY

Effective Date: [TO BE CONFIRMED]

Selfie / Liveness Verification:

- A clear selfie photograph of the client holding their identity document next to their face, OR
- Completion of an automated liveness verification check through the Company's verification platform

[COUNSEL TO REVIEW: Confirm the acceptability criteria for identity and address documents under Saint Lucia AML regulations. Assess whether biometric liveness checks satisfy regulatory requirements for non-face-to-face onboarding.]

3.2 Corporate Clients

Where the applicant is a legal entity, the Company shall require:

- Certificate of incorporation or registration
- Memorandum and articles of association (or equivalent constitutional documents)
- Register of directors and shareholders
- Identification and verification of all directors and beneficial owners holding 25% or more of the entity's shares or voting rights
- Proof of registered address and principal place of business
- Board resolution authorising the opening of a trading account and designating authorised signatories
- Details of the entity's business activities, source of funds, and purpose of the trading account

[COUNSEL TO REVIEW: Confirm corporate client onboarding requirements under Saint Lucia legislation.]

4. ENHANCED VERIFICATION

The Company may require additional documentation or information in the following circumstances:

- The client is identified as a Politically Exposed Person (PEP), a family member of a PEP, or a close associate of a PEP
- The client is a resident of a jurisdiction assessed as high-risk by the FATF, CFATF, or the Company's own risk assessment
- The client's deposit or withdrawal activity exceeds certain thresholds [SPECIFY: e.g., cumulative deposits exceeding $10,000]
- The Company has reasonable grounds to doubt the authenticity or adequacy of previously submitted documents
- The client's trading or transaction pattern raises concerns

Enhanced verification measures may include:

- Certified or notarised copies of identity and address documents
- Bank reference letter from a recognised financial institution
- Declaration of source of wealth and source of funds
- Additional identity documents (e.g., second form of government-issued ID)
- Video verification call with a compliance officer

5. VERIFICATION PROCESS AND TIMEFRAMES

5.1 The Company will endeavour to complete verification within [SPECIFY: e.g., 1-3 Business Days] of receiving all required documents in a satisfactory format.

5.2 Where documents are unclear, incomplete, or require further review, the Company may request resubmission or additional documentation. In such cases, the verification timeframe will be extended until satisfactory documentation is received.

5.3 The Company uses automated verification technology and manual review by trained compliance personnel. The Company may also engage third-party verification providers to assist with identity and document verification, sanctions screening, and PEP checks.

6. ACCOUNT RESTRICTIONS DURING PENDING VERIFICATION

6.1 Until KYC verification is satisfactorily completed:

- The Client may be permitted to deposit funds only, subject to a deposit limit of [SPECIFY: e.g., $2,000]
- Trading, order placement, and withdrawals of funds will not be permitted
- The Company may impose additional account restrictions at its discretion

6.2 If the Client fails to complete KYC verification within [SPECIFY: e.g., 30 calendar days] of opening their Account, the Company reserves the right to suspend or close the Account and return any deposited funds to the original source of deposit.

[COUNSEL TO REVIEW: Confirm that the deposit-only-pending-verification model is aligned with Saint Lucia AML/CDD requirements, including the CDD-before-relationship rule in the Anti-Money Laundering Policy, and that the proposed deposit cap is appropriate.]

7. RE-VERIFICATION AND ONGOING DUE DILIGENCE

The Company may require clients to re-verify their identity and/or address in the following circumstances:

- The client's identity documents have expired
- The client notifies the Company of a change of name, address, or nationality
- The Company's periodic review of client files identifies outdated or insufficient documentation
- A significant change in the client's trading activity or risk profile is detected
- The client requests changes to their account settings, such as a change of account currency or account type
- As part of a routine periodic review cycle (at least every [SPECIFY: e.g., 24 months])

Failure to provide updated verification documents within the specified timeframe may result in account restrictions or suspension.

8. DATA HANDLING AND PRIVACY

All personal data and documents collected during the KYC process are handled in accordance with the Company's Privacy Policy and applicable data protection laws, including the General Data Protection Regulation (GDPR) for EU/EEA clients.

KYC documentation is stored securely using encryption and access controls. Retention of KYC records is governed by the Company's Anti-Money Laundering Policy (minimum five (5) years after account closure).

The Company may share KYC information with third-party verification providers, regulatory authorities, and law enforcement agencies as required by law.

9. DOCUMENT REJECTION AND APPEAL

9.1 The Company reserves the right to reject any document that does not meet the acceptance criteria set out in this Policy, or where the Company has reasonable grounds to suspect that the document is forged, altered, or otherwise fraudulent.

9.2 Where a document is rejected, the Client will be notified of the reason for rejection and invited to submit an alternative document or to resubmit a corrected version.

9.3 If a Client's KYC application is ultimately declined, the Client may appeal the decision by contacting the Company's compliance team at compliance@noblefxm.com. Appeals will be reviewed by a senior compliance officer, and the Client will be notified of the outcome within [SPECIFY: e.g., 10 Business Days].

9.4 The Company is not obligated to provide detailed reasons for declining a KYC application where doing so could compromise the Company's security measures or ongoing investigations.

10. THIRD-PARTY VERIFICATION PROVIDERS

The Company may engage third-party service providers to perform elements of the verification process, including identity document authentication, facial recognition, liveness detection, sanctions screening, and adverse media checks.

Where third-party providers are used, the Company shall ensure that:

- The provider meets appropriate security and data protection standards
- The provider's processes are consistent with the requirements of this Policy
- The Company retains responsibility for the adequacy of the overall KYC process

[COUNSEL TO REVIEW: Confirm data processing agreements and cross-border data transfer arrangements with third-party verification providers.]

11. POLICY REVIEW

This Policy is reviewed and updated at least annually, or more frequently as required by changes in applicable laws, regulations, or the Company's risk assessment. Questions about this Policy may be directed to compliance@noblefxm.com.