NobleFXM

Anti-Fraud 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

ANTI-FRAUD 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 maintaining the integrity and security of its services and to protecting its clients, partners, and the Company from fraud. This Anti-Fraud Policy ("Policy") sets out the Company's approach to preventing, detecting, investigating, and responding to fraudulent activities.

This Policy applies to all directors, officers, employees, contractors, agents, clients, and partners of the Company.

2. PROHIBITED ACTIVITIES

The following activities are strictly prohibited and constitute fraud or abuse under this Policy:

2.1 Identity Fraud

- Opening an account using false, stolen, or fabricated identity documents
- Assuming the identity of another person for the purpose of opening or operating a trading account
- Providing false or misleading information during the KYC verification process
- Using deepfakes, manipulated photographs, or other deceptive means to circumvent identity verification

2.2 Payment and Financial Fraud

- Depositing funds using stolen credit or debit cards, bank accounts, or payment methods
- Initiating chargebacks or payment reversals after funds have been deposited and used for trading
- Depositing funds from accounts not belonging to the account holder (third-party deposits in violation of the Company's policies)
- Structuring deposits or withdrawals to evade AML reporting thresholds

2.3 Bonus and Promotional Abuse

- Opening multiple accounts to receive multiple bonuses
- Using hedging, arbitrage, or other strategies solely for the purpose of meeting bonus lot requirements without genuine trading intent
- Collusion with other clients to exploit promotional offers
- Systematic exploitation of bonus terms through any means not intended by the Company

2.4 Multi-Accounting

- Operating multiple accounts without the Company's prior written approval
- Using family members, associates, or third parties to open additional accounts for the benefit of the same individual

2.5 Platform and System Exploitation

- Exploiting errors, glitches, or delays in the Company's pricing, execution, or platform systems
- Using latency arbitrage or other high-frequency techniques to exploit infrastructure delays
- Attempting to manipulate market prices or platform functionality through automated systems, scripts, or bots (unless expressly permitted by the Company)
- Reverse-engineering, decompiling, or attempting to extract proprietary algorithms or data from the Company's platforms

2.6 Money Laundering and Terrorist Financing

- Using the Company's services to launder proceeds of crime or to finance terrorism
- Any activity constituting money laundering or terrorist financing as defined in the Company's Anti-Money Laundering Policy

2.7 Insider Trading and Market Manipulation

- Trading on the basis of material, non-public information (insider trading)

- Engaging in market manipulation, including spoofing, layering, or wash trading

3. DETECTION METHODS

The Company may use a combination of automated and manual methods to detect fraudulent activity. Depending on implementation scope and third-party provider availability, these may include:

- Automated transaction monitoring that may flag unusual patterns (e.g., rapid deposits/withdrawals, unusual trading patterns, or multiple account registrations from the same IP or device)
- IP address and device fingerprinting to help detect multi-accounting
- Document verification, including automated authenticity checks and manual review by trained compliance personnel, typically through third-party verification providers
- Sanctions and adverse media screening at onboarding and on an ongoing basis
- Behavioural analysis of trading patterns to identify potential manipulation, arbitrage abuse, or system exploitation
- Chargeback and payment dispute monitoring
- Internal reporting by employees and partners

[COUNSEL TO REVIEW: Confirm which of the above detection methods are operationally implemented at the relevant effective date versus those reflecting planned controls, and align the language accordingly.]

4. INVESTIGATION PROCESS

4.1 Where a potential fraud case is identified, the Company's compliance team will initiate an investigation. The investigation may include:

- Reviewing the client's account activity, documentation, and communication history
- Requesting additional information or documentation from the client
- Engaging third-party forensic or investigation services
- Consulting with law enforcement or regulatory authorities

4.2 The Company will conduct investigations fairly and in a timely manner. Clients under investigation will be notified to the extent permissible by law, but the Company is not obliged to disclose the details of its investigation methodology or findings where doing so could compromise the investigation or the Company's security measures.

5. ACCOUNT FREEZING AND SUSPENSION

5.1 During an investigation, the Company may, at its sole discretion:

- Freeze or suspend the client's account(s), preventing further trading, deposits, and withdrawals
- Restrict access to the client's trading platform(s)
- Place holds on pending withdrawals
- Void or reverse transactions executed as a result of or in connection with the suspected fraudulent activity

5.2 Account freezing is a protective measure and does not constitute a determination of fraud. If the investigation concludes that no fraud occurred, the account will be reinstated and any restrictions removed.

6. CONSEQUENCES OF CONFIRMED FRAUD

Where the Company determines that fraud or abuse has occurred, the Company may take one or more of the following actions:

- Permanent termination of the client's account(s)
- Voiding all profits and bonuses generated through or in connection with the fraudulent activity

- Forfeiture of funds in the account(s) to the extent legally permissible [COUNSEL TO REVIEW: Confirm legal basis for fund forfeiture under Saint Lucia law]
- Recovery of any funds paid out to the client as a result of the fraud (including through chargeback claims, legal proceedings, or debt collection)
- Reporting the matter to law enforcement authorities and regulatory bodies
- Sharing relevant information with other financial institutions, payment providers, and industry fraud databases
- Banning the individual from opening future accounts with the Company

[COUNSEL TO REVIEW: Confirm that each consequence listed above is legally permissible under Saint Lucia law and under the laws of key client jurisdictions. Ensure adequate contractual basis for profit voiding and fund forfeiture.]

7. FUND RECOVERY

Where funds have been obtained from the Company through fraud, the Company will take all reasonable steps to recover those funds, including:

- Initiating chargeback claims with payment providers
- Pursuing civil legal proceedings for recovery of funds
- Cooperating with law enforcement in criminal proceedings
- Engaging debt collection agencies

8. COOPERATION WITH LAW ENFORCEMENT

The Company cooperates fully with law enforcement agencies, regulatory authorities, and financial intelligence units in the investigation and prosecution of fraud. The Company will share information and provide access to records as required by law or as necessary to support investigations.

9. CLIENT OBLIGATIONS

Clients are expected to:

- Provide accurate and truthful information at all times
- Safeguard their account credentials and not share them with third parties
- Report any suspected fraudulent activity, unauthorised account access, or security breaches to the Company immediately at support@noblefxm.com
- Cooperate with the Company's investigations when requested
- Not engage in any of the prohibited activities set out in Section 2

10. EMPLOYEE AND PARTNER OBLIGATIONS

All employees, contractors, and partners of the Company are required to report any suspected fraud or policy violations to the compliance team. The Company maintains a confidential reporting mechanism for internal reports. No employee or partner shall suffer retaliation for making a good-faith report of suspected fraud.

11. POLICY REVIEW

This Policy is reviewed at least annually and updated as necessary to reflect changes in fraud typologies, technology, regulations, or the Company's operations. Questions about this Policy may be directed to compliance@noblefxm.com.