STRYKE MARKETS

Anti-Money Laundering (AML) Policy

Effective Date: February 01, 2026

1. Introduction

Stryke Markets Ltd. (the “Company”, “we”, “us”, “our”) is committed to preventing and actively combating money laundering, terrorist financing, fraud, and other illicit financial activities. The Company adopts a risk-based approach in accordance with internationally accepted standards for anti-money laundering and counter-terrorist financing (“AML/CFT”).

This Policy describes the internal controls, procedures, and governance framework implemented by the Company to identify, monitor, and mitigate AML-related risks while providing clients with efficient access to trading services.

2. Scope of Application

This AML Policy applies to:

- All clients and trading accounts maintained by the Company;
- All deposits, withdrawals, and trading activity;
- All employees, directors, officers, consultants, agents, and contractors;
- All affiliates, introducing brokers, and partners acting on behalf of the Company.

3. Regulatory & Risk-Based Framework

The Company applies a risk-based approach to AML compliance, meaning compliance measures are proportionate to the level of risk identified.

This approach considers:

- Client profile and jurisdiction;
- Transaction behavior and volume;
- Payment method used;
- Operational and delivery channels.

The Company reserves the right to enhance or restrict services depending on the assessed risk level.

4. Customer Identification & Verification (KYC)

4.1 Prior to opening an account or permitting withdrawals, clients must complete identity verification procedures. These typically include:

- A valid government-issued photo identification document; and
- Proof of residential address issued within a reasonable timeframe.

4.2 Corporate or legal-entity clients may be required to provide documentation verifying:

- Legal existence;
- Ownership and control structure;
- Authorized representatives.

4.3 The Company may request additional documentation where necessary to meet compliance obligations or mitigate identified risks.

5. Ongoing Due Diligence & Monitoring

5.1 The Company conducts ongoing monitoring of client activity to ensure transactions are consistent with the Company's knowledge of the client and expected account usage.

5.2 Monitoring includes, but is not limited to:

- Deposit and withdrawal behavior;
- Frequency and timing of transactions;
- Changes in payment methods or jurisdictions;
- Activity inconsistent with prior account patterns.

5.3 Where anomalies or irregularities are detected, the account may be flagged for enhanced review.

6. Deposits, Withdrawals & Third-Party Payments

6.1 All deposits and withdrawals must be made using payment methods registered in the client's own name.

6.2 Third-party payments, including funding or withdrawals involving persons or entities other than the verified account holder, are strictly prohibited.

6.3 Where practicable, withdrawals are returned to the original source of deposited funds.

6.4 The Company reserves the right to delay, hold, refuse, or reverse transactions pending completion of compliance checks or resolution of concerns.

7. Sanctions, PEPs & Restricted Jurisdictions

7.1 The Company does not accept clients from, or facilitate transactions involving, jurisdictions subject to international sanctions, embargoes, or legal restrictions.

7.2 Client screening may include checks against:

- Sanctions lists;
- Politically Exposed Persons (PEP) databases;
- Adverse media sources.

7.3 Matches or potential matches may result in enhanced review, account restriction, or termination.

8. Suspicious Activity Identification & Response

8.1 Indicators of potentially suspicious activity may include:

- Rapid deposits followed by immediate withdrawals;
- Structuring transactions to avoid thresholds;
- Repeated changes in payment details;
- Use of multiple accounts without clear justification.

8.2 If suspicious activity is identified, the Company may:

- Request additional information or clarification;
- Restrict or suspend account activity;
- Terminate the client relationship.

8.3 The Company reserves the right to report suspicious activity to appropriate authorities where required by law.

9. Record Keeping & Data Retention

9.1 The Company maintains records relating to client identification, transaction history, and compliance actions in a secure manner.

9.2 Records are retained for a minimum period in accordance with applicable legal and regulatory requirements or internal policy.

10. Governance & Oversight

10.1 The Company appoints an AML Compliance Officer (“AMLCO”) responsible for the implementation and oversight of this AML Policy.

10.2 A Money Laundering Reporting Officer (“MLRO”) is designated as the primary internal point of contact for reviewing and escalating suspicious activity.

10.3 The AMLCO and MLRO report directly to senior management and operate independently from revenue-generating functions.

11. Employee & Affiliate Training

11.1 All relevant employees, contractors, and affiliates receive AML training upon onboarding and at least annually thereafter.

11.2 Training includes:

- AML risk awareness;
- Identification of suspicious activity;
- Sanctions compliance;
- Internal escalation procedures.

11.3 Personnel must acknowledge that they have read, understood, and will comply with this AML Policy.

12. Independent Review & Policy Maintenance

12.1 The Company periodically reviews the effectiveness of its AML framework and internal controls.

12.2 This Policy may be updated to reflect changes in risk profile, business operations, or regulatory expectations.

13. Amendments

The Company reserves the right to amend or restate this AML Policy at any time.

Updated versions will be published on the Company's website. Continued use of the Company's services constitutes acceptance of the revised Policy.

14. Client Acknowledgement

By opening an account and using the Company's services, clients acknowledge that:

- Identity verification is required;
- Transactions are monitored;
- Failure to comply with AML requirements may result in account restriction or termination.