Anti-Money Laundering (AML) Policy

FuryFortuna Ltd - Anti-Money Laundering (AML) & KYC Policy

Version 2.0 - Effective September 2026 - Supersedes all prior versions

1. Policy Statement & Scope

1.1 Purpose & Commitment

FuryFortuna Ltd ("FuryFortuna", "the Company", "we", "us") is dedicated to upholding the highest international standards of Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT), Countering Proliferation Financing (CPF), and Know Your Customer (KYC) compliance.

The purpose of this Policy is to prevent FuryFortuna trading platforms and payment gateways from being utilized for money laundering, terrorist financing, proliferation financing, sanctions evasion, tax evasion, fraud, or financial crime.

1.2 Legislative & Regulatory Alignment

This Policy is formulated in strict accordance with:

- The Money Laundering (Prevention) Act, Cap. 12.20 of the Revised Laws of Saint Lucia (2023 Revision), as amended, including by Act No. 18 of 2024 (the "MLPA"), and the Money Laundering (Prevention) Regulations, 2023 (S.I. No. 53 of 2023), as amended (the "Regulations").
- The Proceeds of Crime Act, Cap. 3.04 of Saint Lucia.
- The Anti-Terrorism Act, Cap. 3.16 of Saint Lucia, as amended.
- The United Nations Sanctions (Counter-Proliferation Financing) Act, Cap. 12.30 of Saint Lucia.
- The Data Protection Act of Saint Lucia, in respect of the processing and retention of personal data.
- The international standards and recommendations established by the Financial Action Task Force (FATF) and the Caribbean Financial Action Task Force (CFATF).
- Guidance notes, guidelines and directions issued by the Financial Intelligence Authority (FIA) of Saint Lucia.

2. Customer Due Diligence (CDD) & KYC Standards

FuryFortuna enforces a risk-based Customer Due Diligence (CDD) framework using automated verification technology (including SumSub / ShuftiPro) to verify client identities, perform biometric liveness checks, and conduct real-time screening against global risk databases. The Company remains fully responsible for the adequacy of all customer due diligence performed using third-party technology, and all verification

records must be retrievable without delay (regulations 6 and 34 of the Regulations).

2.1 Automated Pre-Registration Screening

Prior to account activation or accepting initial deposits, all user registration details are automatically screened against global Sanctions, Politically Exposed Persons (PEP), and Adverse Media watchlists.

- Match Protocol: Any applicant generating an unresolvable match is flagged for mandatory KYC verification prior to depositing funds.
- Clear Protocol: Applicants passing initial screening without risk flags may, where eligible under Section 2.2, proceed to deposit funds under the Express Trading (Delayed CDD) framework, subject to all conditions in that Section.

2.2 Delayed Customer Due Diligence (Express Trading Facility)

In accordance with section 17(12) of the MLPA and regulation 32 of the Regulations, natural persons who successfully pass initial automated pre-screening may be granted access to an interim Express Trading facility prior to completing full documentary verification, subject to the following conditions:

Legal Basis & Management Approval: Verification may be completed after the business relationship is established only where:

1. This is essential not to interrupt the normal conduct of business, given the non-face-to-face, digital onboarding of retail trading clients;
2. The money laundering, terrorist financing and proliferation financing risks are effectively managed through the limits and restrictions in this Section; and
3. Verification is completed as soon as reasonably practicable.

The Express Trading framework, including its limits, must be approved in advance by the Board of Directors and senior management, which is intended to constitute the management approval required by regulation 32(2)(b) of the Regulations. Its operation is subject to regular sampling review by the Compliance Officer.

- Eligibility: Express Trading is strictly limited to individual retail clients classified as Low Risk. Corporate legal entities, Politically Exposed Persons (PEPs), applicants residing in FATF-monitored jurisdictions, and high-risk applicants are strictly ineligible and must complete full verification prior to funding or trading.
- Cumulative Funding Ceiling: Total cumulative deposits across all trading accounts under the client profile shall not exceed $9,999.00 USD (or account currency equivalent). Any deposit or cumulative funding that reaches or exceeds $10,000.00 USD requires upfront completion and approval of Full KYC verification before funds can be credited.
- Verification Deadline: The client must submit complete, valid identity and address verification documentation within thirty (30) calendar days from the date of their initial deposit.

- Strict Withdrawal Restriction: Outbound withdrawals, internal account transfers, and profit distributions are strictly prohibited while an account remains in Express Trading status. Withdrawals will only be unlocked upon official approval of full identity verification.
- Automated Close-Only Enforcement: If full verification is not approved within thirty (30) calendar days of the initial deposit, or before any deposit would cause cumulative deposits to reach US$10,000.00 (or currency equivalent):
  - All associated trading accounts will automatically transition to Close-Only mode (the client may close existing positions, but opening new orders will be disabled).
  - Further incoming deposits will be blocked.
  - Full platform functionality will remain restricted until complete verification is approved by the Compliance Department.
- Termination for Failure to Complete CDD: Where full verification has not been approved within forty-five (45) calendar days of the initial deposit, the business relationship is terminated in accordance with section 17(6) of the MLPA and regulation 33 of the Regulations. Before termination, the Compliance Officer considers and documents whether a Suspicious Transaction Report is required. Where there is no suspicion, the client may close open positions, and the remaining balance is returned only to the verified originating source of funds. Where there is suspicion, the reporting obligations in Section 6.2 apply, no funds are released

without considering any direction or guidance from the FIA, and the client is not informed of any report.

2.3 Individual Verification Standards & Anti-Circumvention Controls

To satisfy statutory Customer Due Diligence mandates, individual applicants must complete identity verification via the Company's secure digital verification framework:

- Proof of Identity (POI) & Biometric Liveness:
  - Applicants must submit a valid, government-issued photo identification document (International Passport, National Identity Card, Residence Permit, or Photo Driver's License) accompanied by a real-time 3D biometric liveness check.
  - Document Validity: Submitted identification documents must have a minimum remaining validity of at least thirty (30) calendar days at the time of submission. Documents expiring in less than 30 days will not be accepted.
- Proof of Residential Address (POA):
  - Applicants must submit an official document verifying their residential address (Utility Bill, Bank or Credit Card Statement, or Local Government Tax Notice) issued within the last ninety (90) calendar days, displaying their full legal name and physical address (P.O. Boxes are strictly prohibited). Where supported, digital electronic address validation may be utilized.
- Economic Baseline & Source of Funds:
  - All applicants must complete a financial profile declaration regarding employment status, industry sector, primary

source of trading capital, and anticipated deposit volume, accompanied by a formal attestation confirming that all funds originate from lawful activities. Documentary evidence of source of funds is obtained where cumulative deposits reach US$10,000.00 (or currency equivalent), where activity is inconsistent with the declared profile, and in all EDD cases. Clients complete any source of funds declaration prescribed under section 21 of the MLPA where that section applies.

- Anti-Circumvention & Security Controls:
  - To prevent synthetic fraud, bot activity, and jurisdictional circumvention, online identity verification must be completed using a genuine, direct local internet connection. Verification sessions initiated through Virtual Private Networks (VPN), proxies, Tor networks, or anonymizing relay services are strictly prohibited and will be rejected.
- Document Expiration Lifecycle & Grace Period:
  - Clients are notified prior to the expiration of their identification documents.
  - Upon document expiration, withdrawal functionality is immediately locked to maintain compliance.
  - To minimize trading disruption, clients are granted a thirty (30) calendar day grace period post-expiration during which existing trading positions may continue to be managed.
  - If an updated, valid document is not approved within 30 days following expiration, the account will automatically

transition to Close-Only mode and new deposits will be blocked.

2.4 Corporate Legal Entity Verification (KYB Framework & Zero Delayed CDD)

Corporate legal entities present distinct financial crime and layering risks. FuryFortuna strictly enforces a Zero Delayed CDD Mandate for all corporate accounts. No legal entity may deposit funds, execute trades, or initiate transfers until full KYB verification is approved.

- Ultimate Beneficial Ownership (UBO) Identification:
  - Standard Structures (≥ 25%): Full identity verification is mandatory for every natural person who directly or indirectly owns or controls 25% or more of the shares, voting rights, or capital of the entity.
  - High-Risk & Multi-Layered Structures (≥ 10%): For corporate entities incorporated in, operating in, or owned through offshore financial centers, complex multi-tier holding entities, or higher-risk jurisdictions, the UBO verification threshold is strictly lowered to 10% or more direct or indirect ownership.
  - Control Through Other Means: Where the ownership test does not identify a natural person, or there is doubt whether the person holding the ownership interest is the beneficial owner, the Company identifies any natural person exercising control of the entity through other means (including powers to appoint or remove the majority of the board, powers of attorney, or contractual or convertible rights).

    - Persons on Whose Behalf Transactions Are Conducted: The Company identifies the individual on whose behalf any transaction or activity is being conducted (MLPA, section 2, definition of "beneficial owner", paragraph (d), as inserted by Act No. 18 of 2024).
    - Senior Managing Officials: Where no natural person is identified under the ownership or control tests above after exhaustive examination, the identity of the Senior Managing Official (e.g., Chief Executive Officer or Managing Director) must be verified. Nominee directors may not be treated as the Senior Managing Official.

- Required Corporate Dossier: Applying entities must provide certified copies of the Certificate of Incorporation, Memorandum and Articles of Association (or Bylaws), Certificate of Good Standing or Incumbency (mandatory for entities registered over 12 months), Register of Directors, Register of Shareholders, Proof of Operating Address, and a formal Board Resolution authorizing account opening and designating authorized signatories.
- Individual Verification for Key Personnel: Full identity, address, and biometric verification is required for all declared UBOs, at least two Directors (all Directors for High Risk entities), and all authorized account signatories and traders.
- Prohibition of Bearer Shares: Entities that have issued bearer shares are strictly prohibited from opening an account, unless all such shares have been immobilized with an approved regulatory custodian.

- Trusts, Foundations & Other Legal Arrangements: Where the applicant is, or is owned through, a trust, foundation or similar legal arrangement, the Company identifies and verifies the settlor(s) or founder(s), trustee(s) or council members, protector (if any), beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control, looking through any legal person acting in such a role to its own beneficial owners, in accordance with FIA guidance on the identification and verification of beneficial owners.

3. Risk-Based Approach (RBA) & Enhanced Due Diligence (EDD)

FuryFortuna employs a comprehensive Risk-Based Approach to assess, categorize, and mitigate financial crime risk across all client relationships. Every profile is dynamically evaluated based on geographic jurisdiction, automated background screening results, economic profile, and transaction activity.

3.1 Risk Categories & Operational Impact

- Low & Medium Risk: Subject to standard customer due diligence and ongoing transaction monitoring. Periodic profile re-verification is conducted at least every 36 months for Low Risk clients and every 24 months for Medium Risk clients, and upon trigger events (including material changes in activity, profile information or risk rating).
- High Risk: Triggers mandatory upfront Enhanced Due Diligence (EDD). Express Trading is strictly unavailable. High-

risk clients must submit documentary evidence verifying their Source of Wealth (SOW) and Source of Funds (SOF) (such as audited accounts, tax returns, bank statements, or asset sale agreements) and obtain formal approval of senior management and the Compliance Officer prior to account activation (regulation 35(2)(c) of the Regulations). High-risk profiles undergo full annual compliance reviews and heightened transaction surveillance.

- Prohibited: Applicants matching active global sanctions lists, confirmed terrorist financing databases, or operating from FATF Blacklisted jurisdictions (Call for Action) are strictly prohibited and immediately blocked from the platform.

3.2 Politically Exposed Persons (PEPs)

A Politically Exposed Person (PEP) is an individual who is or has been entrusted with prominent public functions (e.g., Heads of State, senior politicians, judicial or military officials, senior executives of state-owned corporations), or their immediate family members and close associates. A close associate includes any individual who maintains a close business or personal relationship with a PEP. The definition covers foreign PEPs, domestic PEPs and persons entrusted with a prominent function by an international organisation.

- PEP Screening: Automated screening is conducted at onboarding and continuously monitored against global PEP databases.
- EDD Approval: Opening an account for a PEP requires Senior Management & Compliance Officer approval, reasonable

measures to establish both source of wealth and source of funds, mandatory Enhanced Due Diligence, and enhanced ongoing monitoring of the business relationship.

- Foreign & Domestic PEPs: Enhanced Due Diligence is mandatory for foreign PEPs and their family members and close associates. For domestic PEPs and international organisation PEPs, Enhanced Due Diligence is applied where the relationship is assessed as higher risk (MLPA, section 18).
- Existing Clients: Where an existing client or beneficial owner is identified as, or becomes, a PEP, continuation of the business relationship requires senior management approval.
- Cessation of PEP Status: A person continues to be treated as a PEP for at least two (2) years after ceasing to hold the prominent public function (MLPA, section 18(3)). Thereafter, PEP status is removed only following a documented risk assessment approved by the Compliance Officer.

3.3 Sanctions Screening, Prohibited Jurisdictions & Regional Access Framework

- Real-Time Sanctions Screening: FuryFortuna automatically screens all applicants and existing clients against official global sanctions lists prior to account activation and continuously thereafter. Watchlists evaluated include the United States OFAC, United Nations Security Council Consolidated List (as given effect in Saint Lucia under the Anti-Terrorism Act, Cap. 3.16 and the United Nations Sanctions (Counter-Proliferation Financing) Act, Cap. 12.30), any list of specified entities issued in Saint Lucia, European Union Consolidated List, United Kingdom HM Treasury, and

international law enforcement registers. Any applicant or client identified as an active target on a sanctions list is immediately blocked. All funds and other assets of a designated person are frozen without delay and without prior notice, no funds, assets or services are made available directly or indirectly to or for the benefit of that person, and the matter is reported immediately to the FIA (MLPA, section 16(1)(ka)) and to any other authority as required by the applicable sanctions legislation. Frozen assets remain frozen until delisting or until the competent authority directs otherwise.

- Completely Prohibited Jurisdictions (Strict Exclusion & Account Block): FuryFortuna maintains a zero-tolerance policy and strictly prohibits account creation, receiving deposits, or providing trading services to natural persons residing in or holding citizenship of, as well as legal entities organized under the laws of, jurisdictions subject to comprehensive international sanctions, designated on the FATF High-Risk Call for Action (Blacklist), or otherwise excluded under the Company's risk appetite or for regulatory reasons. Inbound access and registration from the following territories are strictly blocked under all circumstances:
  - Democratic People's Republic of Korea (North Korea - KP): FATF High-Risk Call for Action (Blacklist) / UN & OFAC Sanctions.
  - Islamic Republic of Iran (Iran - IR): FATF High-Risk Call for Action (Blacklist) / Comprehensive International Sanctions.

    - Republic of the Union of Myanmar (Burma - MM): FATF High-Risk Call for Action (Blacklist).
    - Republic of Cuba (Cuba - CU): Comprehensive OFAC Embargo.
    - Syrian Arab Republic (Syria - SY): Comprehensive International Sanctions.
    - Russian Federation (Russia - RU): Comprehensive Financial, SWIFT Restrictions & Regulatory Blacklists.

- FATF Monitored Jurisdictions (Greylist - Mandatory Enhanced Due Diligence): Applicants residing in jurisdictions identified by the FATF as under Increased Monitoring (Greylist) are strictly ineligible for Delayed CDD / Express Trading. Account activation requires mandatory upfront Enhanced Due Diligence (EDD), documentary verification of Source of Wealth and Source of Funds, and formal approval by senior management and the Compliance Officer (MLRO) (regulation 35 of the Regulations). The applicable list is the most recent FATF publication following each FATF Plenary, and screening rules are updated promptly after each publication.
- Non-Solicited Jurisdictions (Reverse Solicitation Regional Gate): To comply with cross-border financial promotion regulations, FuryFortuna does not market, advertise, or actively solicit clients in jurisdictions where derivative distribution or local licensing restrictions apply. The platform maintains automated IP-based disclaimer controls covering 37 Restricted Jurisdictions:
    - Standalone Jurisdictions (7): United States of America (US), Canada (CA), Japan (JP), Singapore (SG), Australia

(AU), United Kingdom (GB), and Saint Lucia (LC).

- European Economic Area (EEA) Member States (30): Austria (AT), Belgium (BE), Bulgaria (BG), Croatia (HR), Cyprus (CY), Czech Republic (CZ), Denmark (DK), Estonia (EE), Finland (FI), France (FR), Germany (DE), Greece (GR), Hungary (HU), Iceland (IS), Ireland (IE), Italy (IT), Latvia (LV), Liechtenstein (LI), Lithuania (LT), Luxembourg (LU), Malta (MT), Netherlands (NL), Norway (NO), Poland (PL), Portugal (PT), Romania (RO), Slovakia (SK), Slovenia (SI), Spain (ES), and Sweden (SE).
- Reverse Solicitation Principle: Registration from these 37 jurisdictions is permitted strictly on the applicant's own exclusive initiative and unsolicited request. Applicants from these territories must pass standard automated pre-screening, complete mandatory legal attestations, and comply with all applicable Customer Due Diligence standards before accessing full trading services. Reliance on reverse solicitation is assessed on the facts and cannot be established by disclaimers, terms and conditions or acknowledgement boxes alone. Any marketing, promotion or solicitation directed at these jurisdictions by the Company or by any introducing broker, affiliate or other person acting on its behalf defeats reliance on this principle. Evidence of client initiative is recorded for each client from these jurisdictions.

4. Payment Method Security, Ownership Verification & Anti-Third-Party Rules

To prevent financial crime, money laundering, and payment layering, FuryFortuna strictly regulates all fund flows:

- Strict Legal Name-Matching: The legal name registered on the FuryFortuna account must match exactly the name on the depositing and receiving financial source (bank account, payment card, or verified cryptocurrency wallet).
- Third-Party Payment Prohibition: Funding from or withdrawing to third parties (including spouses, relatives, business partners, or non-verified commercial entities) is strictly prohibited.
  - Any detected third-party deposit will be frozen immediately and returned exclusively to the originating funding source at the sender's expense, subject to an administrative processing fee of up to US$100, as set out in the Client Agreement. Before any such return, the Compliance Officer assesses whether the deposit gives rise to suspicion; where it does, the reporting obligations in Section 6.2 apply before any funds are returned, and the client is not informed of any report.
- Cryptocurrency Wallet Proof of Ownership: When submitting or registering a cryptocurrency withdrawal destination, the client must provide verifiable proof of ownership (such as a screenshot or account statement from their private wallet or verified exchange account confirming the wallet address, blockchain network, and the client's legal name). Where the wallet is unhosted or the client is High Risk, ownership must additionally be evidenced by a signed message or a micro-transaction test from the registered address. Incoming and

outgoing virtual asset transfers are subject to blockchain analytics screening or equivalent controls; funds traced to mixers, darknet markets, sanctioned addresses or other high-risk sources are rejected or frozen and escalated to the Compliance Officer.

- Cross-Account Payment Security: To prevent unauthorized financial intermediation, money mule operations, and fund pooling, each payment method and cryptocurrency destination may only be linked to a single verified client profile. Payment destinations cannot be shared across multiple client accounts.
- Statutory Record Retention of Funding Methods: In accordance with international AML recordkeeping standards and Saint Lucia law, the Company maintains an audit trail of all historical funding and withdrawal methods for at least seven (7) years from the end of the business relationship (MLPA, section 16(7)). Saved payment methods cannot be deleted from compliance archives during the applicable retention period; clients may manage their active interface by archiving unused methods from display.

5. Ongoing Monitoring & Red Flag Detection

5.1 Transaction Monitoring

The FuryFortuna Compliance Team utilizes automated monitoring tools to inspect trading patterns, deposit frequencies, and account transfers in real time.

5.2 Red Flag Indicators

The following activities trigger immediate compliance investigation:

- Minimal-Trading Pass-Through: Depositing large sums followed by an immediate request for withdrawal without executing meaningful trading activity (money laundering passthrough).
- Structuring / Smurfing: Making multiple small deposits or withdrawals just below compliance reporting thresholds.
- Unusual Funding Patterns: Funding accounts from multiple disparate geographic locations or unverified crypto mixing services.
- Discrepancies in Information: Inconsistent or altered identification documents during re-verification.
- Multiple Account Operations: Opening multiple accounts using different email addresses or IP ranges to obfuscate identity or trade volume.
- Virtual Asset Risk Indicators: Deposits from or withdrawals to wallets linked to mixers, tumblers, darknet markets, sanctioned addresses or high-risk exchanges, or rapid conversion between assets or blockchains (chain-hopping).
- Sanctions & Proliferation Financing Indicators: Use of intermediaries, addresses, devices or payment instruments linked to designated persons or prohibited jurisdictions or attempts to conceal the origin or destination of funds connected with such jurisdictions.
- Terrorist Financing Indicators: Funding patterns inconsistent with the client's profile involving conflict zones, or links to persons or entities associated with terrorism.

- Alert Handling: Each alert is reviewed promptly and closed with recorded reasons. Escalated cases are referred to the Compliance Officer without delay, and internal review never suspends the statutory reporting deadlines in Section 6.2.

5.3 Account Integrity & Multi-Accounting Controls

Operating multiple accounts under the same personal identity creates significant financial crime, fraud, and market manipulation risks.

- Single Profile Policy: Each natural person or legal entity is permitted to register and operate exactly one (1) master client profile. Attempting to open multiple profiles using alternative email addresses, modified name transliterations, or synthetic identity variations is strictly prohibited.
- Automated Collision Monitoring: The Company utilizes automated identity matching systems to detect duplicate profile registrations. Any registration flagged as a potential duplicate is placed on administrative hold pending compliance review.
- Remedial Action:
  - In the case of inadvertent duplicate registrations, FuryFortuna will consolidate verifiable client funds into the primary master profile and permanently archive the secondary profile.
  - Where multi-accounting is intentionally utilized to circumvent compliance restrictions, engage in abusive trading, or obscure fund origins, FuryFortuna reserves the right to immediately freeze all associated accounts, nullify

illegitimate profits, and terminate the business relationship.

6. Suspicious Transaction Reporting (STR) & FIA Obligations

6.1 Internal Reporting

Any employee, officer, or system alert identifying suspicious activity must promptly escalate an internal Suspicious Activity Report (SAR) to the designated Compliance Officer (acting as Money Laundering Reporting Officer, "MLRO"). Staff must not alert the client or conduct their own further enquiries. Where the Compliance Officer is uncertain whether the facts substantiate a suspicion, a report is made to the FIA (regulation 15(6) of the Regulations).

6.2 External Reporting to Saint Lucia FIU

- Formal STR Submission: If the MLRO determines that reasonable grounds exist to suspect or know that a transaction, series of transactions, or attempted transaction involves funds derived from money laundering, terrorist financing, or criminal activity, a formal Suspicious Transaction Report (STR) shall be submitted to the Financial Intelligence Authority (FIA) of Saint Lucia as soon as reasonably practicable, and in any event within seven (7) days of the transaction being deemed suspicious (MLPA, section 16(1)(k)). Internal review shall not delay this deadline. Any suspicious transaction or attempted transaction relating to terrorist

financing or proliferation financing is reported to the FIA immediately (MLPA, section 16(1)(ka)). Reports are made in the form and manner prescribed by the FIA.

- Prohibition of Tipping-Off: Pursuant to sections 16(3), 16(4) and 33 of the MLPA, FuryFortuna directors, owners, officers, employees and representatives are strictly prohibited from disclosing to the Client or any third party that a SAR/STR has been raised, an internal investigation is underway, or an STR has been filed with the FIA ("Tipping-Off"). Tipping-off is a criminal offence punishable by substantial fines and imprisonment.
- Records of Decisions: The Compliance Officer documents every internal report received, the analysis performed and the decision whether or not to file an STR, with reasons. These records are retained in accordance with Section 7.1.

7. Record Keeping & Staff Training

7.1 Record Retention Period

- Retention Timeline: FuryFortuna maintains all records relating to customer due diligence (including POI, POA, and verification logs), trading account files, financial transaction records, compliance monitoring logs, and internal/external suspicious activity reports for a minimum period of seven (7) years, and for longer where the FIA notifies the Company that records may be relevant to an investigation (MLPA, section 16(6)).

- Commencement of Retention Period: For CDD and account profile records, the seven-year statutory retention period commences on the official date of account closure or formal termination of the business relationship. For transactional records, the retention period commences from the date on which the specific transaction was completed.

7.2 Compliance Training

- Staff Training: All FuryFortuna personnel undergo mandatory training within thirty (30) days of appointment and at least annually thereafter, covering AML/CFT/CPF laws, targeted financial sanctions (including United Nations Security Council Resolutions), red flag detection, customer due diligence procedures, and reporting protocols.
- Specialized Officer Training: The Compliance Officer and the alternate Compliance Officer receive more extensive, role-specific training. Training content, attendance and assessment results are recorded and retained (regulations 9 and 29 of the Regulations).

8. Governance, Compliance Officer & Control Framework

8.1 Board of Directors & Senior Management

The Board of Directors approves this Policy and any material amendment, sets the Company's financial crime risk appetite, approves the Express Trading framework, and receives the Compliance Officer's reports at least quarterly (regulation 26 of

the Regulations). Senior management is responsible for implementing this Policy and for allocating adequate resources to the compliance function.

8.2 Compliance Officer (MLRO)

- Appointment: The Company appoints a Compliance Officer at management level who is a fit and proper person. Where the Company is a reporting entity under the MLPA, the appointment is subject to FIA approval (section 16(1)(n), as amended by Act No. 18 of 2024) and the Compliance Officer's details are submitted to the FIA within seven (7) days of appointment (regulation 22(3) of the Regulations).
- Alternate: An alternate Compliance Officer is appointed, and the Compliance Officer and the alternate are not absent at the same time (regulation 24).
- Independence & Reporting Lines: The Compliance Officer acts independently, has unrestricted access to all records, systems and staff, and reports directly to the Board (regulation 25).
- Responsibilities: The Compliance Officer's responsibilities include those set out in regulation 25(2) of the Regulations, including maintaining this Policy, analyzing and reporting suspicious transactions, testing controls, arranging the independent audit, conducting risk assessments, reporting monthly to senior management and quarterly to the Board, and acting as the Company's contact with the FIA.

8.3 Enterprise-Wide Risk Assessment & New Technologies

The Company maintains a documented enterprise-wide assessment of its money laundering, terrorist financing and proliferation financing risks, covering customers, jurisdictions, products, transactions and delivery channels. It is reviewed at least annually and approved by the Board (MLPA, section 16B; regulation 11(2)(g) of the Regulations). Before launching or using any new product, business practice, delivery channel or technology, including changes to the Express Trading framework, virtual asset payment methods or verification providers, the Company performs and documents a risk assessment (regulation 37).

8.4 Independent Audit

The AML/CFT/CPF programme is independently audited at least annually by a suitably qualified external professional or by an internal auditor who is not involved in the compliance function. Findings are reported to the Board, and any violations are reported to the Board immediately (regulation 13 of the Regulations).

8.5 Employee Screening & Integrity

Before an offer of employment is made, the Company verifies references and academic and professional qualifications and obtains a police certificate of character. It maintains a code of ethics and ongoing integrity measures (MLPA, section 16(1)(o); regulation 28 of the Regulations).

8.6 Outsourcing & Third-Party Verification Providers

Where the Company uses third-party technology or service providers for identity verification, screening or monitoring, it remains fully responsible for compliance with its legal obligations, conducts due diligence on and oversees each provider (including payment service providers and banking partners through which client funds are processed), and ensures that all records are retrievable without delay on request by the FIA (regulations 6 and 34 of the Regulations).

8.7 Cooperation with Authorities & Data Protection

The Company cooperates fully with the FIA and other competent authorities, responds to lawful requests and directions within the timeframes specified, and complies with the Data Protection Act in processing personal data, without prejudice to its AML/CFT/CPF retention and reporting obligations.

8.8 Policy Review

The Compliance Officer reviews this Policy at least annually, and earlier upon any material legislative, regulatory or business change. Amendments are approved by the Board.