Moonetrix

Policy on Combating Money Laundering and Terrorism Financing

Overview

This Policy on Combating Money Laundering and Terrorism Financing (the “Policy”) outlines the Company's unwavering commitment to preventing the use of its products, services, and platforms for the purposes of money laundering, terrorist financing, and related financial crimes. It is designed to ensure compliance with all applicable international standards and domestic legislation, including but not limited to the Financial Action Task Force (FATF) Recommendations and relevant regulatory authority mandates in each jurisdiction in which the Company operates.

The Policy establishes a robust framework of governance, internal controls, risk management procedures, and reporting obligations to deter, detect, and respond to any attempt to misuse the Company’s infrastructure for unlawful financial activity. The Company is committed to maintaining the highest standards of ethical conduct and regulatory compliance to safeguard the integrity of the global financial system.

Application

This Policy applies to:

- All natural and legal persons who engage or intend to engage with the Company as clients, customers, or counterparties.
- All employees, contractors, consultants, and representatives acting on behalf of the Company.
- All services, platforms, products, and financial transactions offered, facilitated, or processed by the Company.

This Policy shall be read in conjunction with the Company’s Code of Conduct, Information Privacy and Security Policy, and other applicable internal guidelines. It is binding on all relevant parties and non-compliance may result in disciplinary measures, including termination of business relationships, regulatory reporting, and potential legal action.

The Policy is intended to be dynamic and shall be updated as necessary to reflect changes in

laws, regulations, emerging risks, and evolving industry best practices.

Definitions

For the purpose of this Policy, the following terms shall have the meanings set forth below, unless the context explicitly requires otherwise:

1. Money Laundering (ML): The process of concealing or disguising the origins of illegally obtained funds so that they appear to be legitimate. This typically involves multiple stages, including placement, layering, and integration.

2. Terrorism Financing (TF): The act of providing or collecting funds, directly or indirectly, with the intention or knowledge that they will be used, in whole or in part, to carry out terrorist acts, or support terrorist organizations or individuals.

3. Client: Any natural or legal person engaging or intending to engage with the Company for the purpose of using its financial services or products.

4. Know Your Customer (KYC): A set of procedures and due diligence processes used by the Company to verify the identity of clients, assess the legitimacy of their source of funds, and understand their financial behavior to mitigate ML/TF risks.

5. Politically Exposed Person (PEP): An individual who holds or has held a prominent public function, including but not limited to heads of state, senior politicians, judicial or military officials, and their immediate family members or close associates.

6. Risk-Based Approach (RBA): A methodology by which the Company identifies, assesses, and applies proportionate mitigation measures according to the level of ML/TF risk posed by a client, product, or transaction.

7. Enhanced Due Diligence (EDD): Additional verification measures and risk controls applied to clients or transactions deemed to carry a higher risk of ML/TF, including PEPs or those from high-risk jurisdictions.

8. Suspicious Transaction Report (STR): A report submitted by the Company to the appropriate regulatory authority upon identification of a transaction or client behavior that raises reasonable grounds to suspect involvement in ML/TF or other financial crimes.

9. Anonymous Client: A client whose true identity cannot be reliably verified through KYC procedures. The Company does not permit business relationships with such individuals or entities.

10. High-Risk Jurisdiction: A country or territory identified by credible sources such as FATF or national authorities as having deficiencies in its AML/CTF frameworks or presenting elevated ML/TF risk.

Moonetrix

Part A: Regulatory Compliance and Corporate Governance

Section 1.1: Regulatory Commitment

The Company acknowledges its legal and regulatory responsibilities under applicable domestic and international anti-money laundering (AML) and counter-terrorism financing (CTF) laws. The Company pledges to cooperate fully and transparently with regulatory bodies and law enforcement agencies in any investigation involving suspicious client activities.

Section 1.2: Compliance Infrastructure

To uphold operational integrity, the Company maintains comprehensive AML/CTF compliance systems comprising preventive controls, routine risk assessments, and internal governance mechanisms designed to shield the Company's services from misuse by criminal actors.

Section 1.3: Zero Tolerance Policy

The Company enforces a strict zero-tolerance stance toward money laundering, terrorist financing, and related illegal conduct. All personnel must adhere strictly to this Policy, supported by ongoing education, compliance training, and supervisory monitoring.

Part B: Client Identification and Due Diligence

Section 2.1: Know Your Customer (KYC) Procedures

In alignment with KYC mandates, the Company performs thorough identity verification on all prospective and current clients. Engagement with the Company constitutes an undertaking to provide accurate, truthful, and current information.

Section 2.2: Source of Funds Verification

Clients must declare and validate the origin of funds for all transactions. Documentation evidencing the legitimacy of funds will be retained securely in compliance with applicable retention regulations.

Section 2.3: Confidentiality and Information Disclosure

The Company may limit access to or withhold transaction data from individuals or third parties when disclosure could jeopardize ongoing investigations or legal compliance. This withholding shall not apply to disclosures legally mandated under applicable AML/CTF regulations, which are addressed under Section 2.4.

Section 2.4: Authorization for Data Use and Reporting
Clients consent to the collection, storage, and lawful disclosure of financial data to relevant authorities, including the submission of Suspicious Transaction Reports (STRs) when warranted by legal requirements.

Section 2.5: Uniform Application of Standards

All clients are subject to a baseline verification standard. The Company may, where permitted by law, apply proportionate enhanced or simplified due diligence based on risk classification.

Section 2.6: Legal Capacity Assessment

The Company reserves the right to evaluate a client's legal capacity to enter into financial agreements and may terminate relationships with clients deemed legally incapacitated.

Part C: Risk-Based Approach and Transaction Monitoring

Section 3.1: Risk Classification and Enhanced Due Diligence

The Company applies a risk-based methodology to client onboarding and monitoring. Enhanced due diligence (EDD) applies to higher-risk clients such as politically exposed persons (PEPs), clients from high-risk jurisdictions, or those exhibiting suspicious transactional conduct.

Section 3.2: Simplified Due Diligence for Low-Risk Clients

Where clients pose minimal risk, the Company may apply proportionate simplified due diligence measures consistent with regulatory standards, subject to periodic reassessment.

Section 3.3: Prohibition on Anonymous Clients and Valid Representation

Anonymous or fictitious client relationships are strictly prohibited. Representation by a third party requires verifiable and legally valid authorization such as a power of attorney.

Section 3.4: Enforcement of Compliance Requirements

The Company reserves the right to refuse, suspend, or terminate transactions or client engagements that do not satisfy documentation or compliance criteria, consistent with procedures outlined in Section 4.3

Section 3.5: Comprehensive Risk Assessment Criteria

Risk assessments incorporate client business profiles, organizational structures, jurisdictional risks, and transactional patterns. Engagement in financing terrorism or prohibited activities results in immediate termination and notification to authorities.

Section 3.6: Regular Internal Audits

Periodic internal audits are conducted to evaluate the effectiveness of AML/CTF controls, including transaction reviews, personnel compliance interviews, and system integrity testing.

Part D: Ongoing Monitoring, Record Management, and

Enforcement Section 4.1: Continuous Account Surveillance

Client accounts and transactional activities are continuously monitored against defined criteria and global watchlists to identify and address irregular or suspicious behavior promptly.

Section 4.2: Data Retention and Secure Disposal

Financial and due diligence records are retained according to legal mandates and securely destroyed or anonymized upon expiration of retention periods.

Section 4.3: Response to Suspicious Activities

Upon detection of suspicious conduct, the Company will take immediate action including freezing accounts, suspending services, and reporting to competent authorities as required by law.

Section 4.4: Whistleblower and Reporting Obligations

Employees and agents are obligated to report known or suspected violations of this Policy. The Company ensures protection for whistleblowers in accordance with relevant laws and conducts impartial investigations.

Section 4.5: Policy Updates and Communication

The Company reserves the right to amend this Policy at its discretion. Significant amendments will be published and communicated through official channels. Continued use of services signifies acceptance of any revisions.

Section 4.6: Legal Interpretation and Consequences of Non-Compliance

This Policy is governed by applicable AML and CTF legislation and is subject to amendment

in response to legal, regulatory, or risk-based developments. Non-compliance may result in termination of services, regulatory reporting, and potential legal proceedings