onequity

AML/CFT Policy

AUGUST 2025

OnEquity (MU) Ltd
FSC License
No. GB23201814

1. Introduction

1.1. Entity and Regulatory Framework: **ONEQUITY (MU) LTD** (the "Company", "We" "OnEquity") is regulated by the Financial Services Commission Mauritius ("FSC") under license number GB23201814 as an Investment Dealer (Full Service Dealer, Excluding Underwriting) and is subject to the Anti Money Laundering and -Counter Financing- of Terrorism regime of the Republic of Mauritius. The AML/CFT Manual is designed to assist OnEquity (MU) Ltd in meeting its obligations under the Financial Intelligence and Anti-Money Laundering Act ('FIAMLA') and the Financial Intelligence and Anti-Money Laundering Regulations ('FIAML Regulations 2018')

1.2. Purpose: This Policy sets out the Company's commitments to prevent, detect and report money laundering and terrorist financing, and establishes internal responsibilities, controls, and procedures consistent with FATF Recommendations.

1.3. Scope: This Policy applies to all business units, employees, contractors and affiliates when performing activities for or on behalf of the Company.

2. Definitions

Unless the context requires otherwise, terms have the meanings commonly used in Mauritius' AML/CFT legislation and FATF terminology, including:

- The Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA)
- Financial Intelligence and Anti-Money Laundering Regulations 2018 (FIAML Regulation 2018)
- The Prevention of Corruption Act 2002
- The Prevention of Terrorism Act 2002
- AML-CFT Handbook
- The Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019

- The Anti Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2020

- The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019

"AML/CFT Compliance Officer": individual appointed under the Regulations with responsibility for compliance and reporting duties.

"Beneficial Owner": the natural person(s) who ultimately owns or controls a legal person/arrangement or on whose behalf a transaction is conducted, whether ownership/control is direct or indirect.

"Business Relationship": a professional or commercial relationship with an element of duration expected by the Company at onboarding.

"Customer Due Diligence (CDD) Measures": identification and verification of the customer and, where applicable, third parties and beneficial owners; understanding the purpose and intended nature of the relationship/transaction; and ongoing monitoring.

Other defined terms include Director; PEP (domestic/foreign/international organization); Intermediary; Introducer; Legal Person; One-off Transaction; Ongoing Monitoring; and Relationship Information.

3. Client Acceptance and Customer Due Diligence

3.1. General: The Company obtains CDD information for every customer, relevant third party and beneficial owner, and verifies identity using reliable, independent sources before establishing a Business Relationship or executing a One-off Transaction.

3.2. Timing: CDD must be completed prior to onboarding or transaction execution. In limited, low risk cases where business continuity requires, verification may be completed as soon as practicable after initial contact; failure to complete verification will result in relationship termination.

3.3. Triggers: CDD is refreshed when doubts arise as to the adequacy or veracity of documents/data, when conducting ongoing monitoring, or when there are changes to identification information, beneficial ownership, or third party arrangements.

3.4. Ongoing Monitoring: The Company scrutinizes transactions to ensure consistency with the customer's profile and keeps CDD information up to date on a risk sensitive basis, with at least annual review for low risk customers. If ongoing monitoring cannot be performed, the relationship will be terminated.

4. Risk Based Approach

4.1. Application:

The Company applies a risk sensitive approach to determine the extent/nature of CDD and ongoing monitoring for each relationship/transaction.

4.2. Assessment:

For each customer, the Company prepares and records a risk assessment considering customer, product/service, delivery channel, and country/geographic risks, and updates it periodically based on new information.

4.3. Enhanced Measures:

Enhanced due diligence and enhanced ongoing monitoring are applied where higher risks exist (e.g., connections to jurisdictions that do not sufficiently apply FATF standards, PEP involvement, private banking, asset holding vehicles, or other higher risk scenarios).

4.4. Non Face to Face:

At least one additional check to mitigate identity fraud is performed and further measures are applied as appropriate.

5. Prohibited or Restricted Accounts

The Company does not approve numbered or anonymous accounts, or accounts in fictitious names, and nominee shareholders/bearer shares.

6. Reliance on Introducers and Intermediaries

6.1. Conditions: The Company may rely on a regulated introducer/intermediary that consents to reliance, provided it obtains immediate access to CDD information and written assurances that: (i) required CDD was performed; (ii) identification evidence is retained; and (iii) records will be provided without delay upon request.

6.2. Assurance & Oversight: Prior to reliance, the Company confirms regulated status and assesses reliance risk to determine whether additional measures are needed. Sufficient information must be obtained to assess ML/TF risk of each introduced customer.

7. Record Keeping

The Company keeps records of risk assessments, CDD information and evidence of identity, relationship/transaction documentation sufficient to reconstruct transactions, account files, and business correspondence, ensuring timely retrieval for competent authorities. Records are maintained to facilitate ongoing monitoring and audits.

8. Policies, Procedures, Systems and controls

The Company maintains risk sensitive policies, procedures, systems and controls addressing CDD and monitoring, reporting, recordkeeping, employee screening, internal controls, risk assessment and management, and compliance oversight and communication.

Identification and scrutiny cover complex/unusually large transactions, unusual patterns without apparent lawful purpose, and other activity potentially related to ML/TF. Additional measures are taken to prevent misuse of products susceptible to anonymity.

Sanctions and High Risk Countries: The Company determines whether customers, third parties or beneficial owners are PEPs, and whether relationships/transactions involve jurisdictions that insufficiently apply FATF standards or are subject to UN/EU/other sanctions.

9. Monitoring, Testing and access to Information

9.1. The Company maintains procedures to monitor and test the effectiveness of AML/CFT policies and training. The AML/CFT Compliance Officer and appropriate staff have timely access to CDD and transaction records necessary to perform their duties.

10. Employee Awareness and Training

10.1. Employees are trained on Company AML/CFT policies and relevant laws, including identification and handling of transactions or behaviours indicative of ML/TF.

11. Risk Based KYC and National/International Context

Risk assessment considers national legal/regulatory frameworks, prescribed significant risks and mitigation measures, and FATF Recommendations. Quantitative and qualitative data (e.g., typologies, red flags, guidance from authorities and inter-governmental bodies) inform the assessment.

12. ML/TF Risk Indicators

Indicators considered include business nature and complexity; proportion of highrisk customers; jurisdictions of operation/exposure (including crime/corruption/TF prevalence, AML/CFT regime, beneficial ownership transparency, supervisory effectiveness); distribution channels and intermediation; technology use; audit and regulatory findings; and expected transaction volumes and sizes.

13. Customer Risk Categorization

13.1. High Risk: Factors may include PEP status (including family/close associates / UBO PEPs); residence or source of wealth in high risk jurisdictions; lack of tax transparency; unwillingness/inability to provide third party/BO documentation; negative media; links to typologies/red flags; unregistered or weakly supervised intermediaries; cash intensive businesses; or regulatory sanctions without remediation. As per the FATF list dated 13 June 2025, customers resident in Algeria, Angola, Bolivia, Bulgaria, Burkina Faso, Cameroon, Côte d’Ivoire, DRC, Haiti, Kenya, Lao PDR, Lebanon, Monaco, Mozambique, Namibia, Nepal, Nigeria, South

Africa, South Sudan, Syria, Venezuela, Vietnam, Virgin Islands (UK), and Yemen are automatically classified as high risk (subject to updates).

13.2. Low Risk: Examples include listed companies subject to robust disclosure; public authorities; customers resident in lower risk jurisdictions with effective AML/CFT; or products with limited services/amounts and transparent ownership (e.g., certain e-money).

13.3. Normal/Medium Risk: Customers not falling within high or low risk categories.

14. Due Diligence for Individuals/Representatives

14.1. At minimum: clear colour copy of a valid passport/official national ID; and proof of permanent residential address (e.g., utility bill, local authority tax bill or bank statement issued within the last six months, showing full name and address). Documents not in English must be accompanied by a translation (dated, signed and stamped by the translator).

14.2. Purpose and Intended Nature: Obtain information sufficient to understand the purpose/intended nature of the relationship; in higher risk cases, obtain additional information to support ongoing monitoring and detect suspicious activity.

14.3. Proportionality: The extent of information and verification increases with risk and may be simplified where risk is demonstrably lower, subject to legal allowances. Risk profiles are periodically updated to calibrate CDD.

15. Due diligence for corporate customers

15.1. Information and Understanding: Obtain sufficient information to understand the customer's business, reputation and supervisory quality, including assessment of AML/CFT controls where appropriate.

15.2. Minimum Documentation (certified true copies): Certificate of Incorporation and Good Standing; Registered Office; Directors/Secretary; Shareholders; Memorandum & Articles; Board Resolution authorizing account opening and operators; trust/nominee documentation where applicable; identification of authorized signatories, registered shareholders and beneficial owners; latest audited financial statements and/or management accounts (if available). The Company may request additional information where necessary.

16. Sanctions Screening

16.1. The Company complies with national and international sanctions legislation. Sanctions screening is mandatory. Where customers (natural or legal) are from sanctioned or very highrisk countries, the Company will not conduct business.

17. Refusal or Termination of Business Relationship

17.1. Where the Company cannot apply CDD prior to establishing a relationship or executing a one-off transaction, it will not proceed. If ongoing monitoring cannot be performed, the relationship will be terminated.

18. Reporting of Suspicious Activity

18.1. Suspicious activity is escalated to the AML/CFT Compliance Officer for consideration and, where appropriate, reported to the competent authority in accordance with applicable laws and guidance.

Note: This Policy must be read in conjunction with applicable Mauritius AML/CFT laws/regulations and FATF standards. Where legislative amendments occur, this Policy shall be interpreted to maintain compliance without altering customer rights or obligations beyond statutory requirements.