UnipayNet

ANTI-MONEY LAUNDERING (AML) POLICY

1. Introduction

1.0 UNIVERSAL PAYMENT NETWORK LIMITED (hereinafter referred to as “the Company”) is fully committed to the highest standards of integrity, transparency, and ethical conduct. The Company recognizes the critical importance of preventing money laundering, terrorist financing, and other forms of illicit financial activity, which pose serious legal, financial, and reputational risks to businesses and the global financial system.

1.1 This Anti-Money Laundering (AML) Policy establishes the Company's comprehensive framework for identifying, mitigating, and managing the risk of financial crime. It outlines the principles, controls, and procedures implemented to detect, prevent, and report suspicious activities, and ensures compliance with all applicable national laws, regulatory requirements, and international standards, including those set forth by the Financial Action Task Force (FATF).

1.2 The Company adopts a zero-tolerance approach to money laundering and is committed to fostering a culture of compliance, vigilance, and accountability at all levels of the organization. This policy is an integral part of the Company’s broader risk management strategy and corporate governance framework.

2. Purpose

2.0 The purpose of this Anti-Money Laundering (AML) Policy is to define the Company’s commitment to establishing and maintaining an effective compliance framework for the prevention and detection of money laundering, terrorist financing, and other related financial crimes.

2.1 This policy outlines the internal controls, procedures, and governance structures necessary to ensure full adherence to applicable anti-money laundering and counter-terrorist financing laws, regulations, and international standards — including the Financial Action Task Force (FATF) Recommendations. It also supports the Company’s strategic objective to safeguard its operations, reputation, and stakeholders by proactively identifying, assessing, and mitigating financial crime risks.

2.2 In doing so, the policy promotes a culture of compliance, accountability, and ethical conduct, and ensures that all employees and stakeholders clearly understand their roles and responsibilities in managing AML risk across all levels of the organization.

3. Scope

This AML Policy applies to all employees, directors, officers, contractors, and agents of the Company, regardless of their location or function. It encompasses all business lines, products, services, and transactions, and is binding across every jurisdiction in which the Company operates. Compliance with this policy is mandatory and integral to the Company's commitment to maintaining the highest standards of legal and regulatory compliance, ethical conduct, and financial integrity.

4. Customer Due Diligence (CDD)
The Company shall conduct thorough customer due diligence (CDD) prior to establishing any business relationship. This includes the identification and verification of all clients, beneficial owners, and controlling parties. Required documentation may include government-issued identification, proof of address, and corporate registration documents.

5. Enhanced Due Diligence (EDD)
For customers and transactions that present a higher risk, the Company will apply Enhanced Due Diligence (EDD) measures. These measures include gathering additional information, conducting background checks, increased monitoring, and obtaining senior management approval prior to proceeding.

6. Ongoing Monitoring
6.0 The Company shall implement a robust, risk-based approach to the ongoing monitoring of all customer relationships and transactions. This process is essential to ensuring that customer activities remain consistent with the Company's knowledge of the client, their business and risk profile, and the nature of the relationship established.

6.1 Monitoring will be both manual and automated, using appropriate systems and tools to detect unusual transaction patterns, red flags, and indicators of potential money laundering or terrorist financing. These systems shall be calibrated to account for various risk levels and will be regularly reviewed and updated to remain effective against evolving threats.

6.2 Ongoing monitoring includes, but is not limited to:

- Regular reviews of high-risk client accounts.
- Continuous evaluation of large, complex, or unusual transactions.
- Detection of transactions that are inconsistent with expected behavior.
- Timely escalation and investigation of identified anomalies.
- Enhanced scrutiny for accounts with high-volume or cross-border activity.

All findings from monitoring efforts must be documented, and any suspicious activity shall be promptly reported to the Money Laundering Reporting Officer (MLRO) for further assessment and, if warranted, reporting to the appropriate authorities.

7. Suspicious Activity Reporting
All employees must report suspicious activities to the designated Money Laundering Reporting Officer (MLRO). The MLRO is responsible for evaluating the

report and, if necessary, submitting a Suspicious Transaction Report (STR) to the appropriate authorities in a timely manner.

8. Record Keeping

The Company shall retain all relevant AML documentation, including customer identification records, transaction histories, and internal reports for at least the minimum period required by law. Records must be readily available for inspection by regulatory authorities.

9. Training and Awareness

All employees will receive ongoing training on AML obligations, the recognition of suspicious activities, and the proper internal reporting procedures. Training programs will be regularly reviewed and updated to remain current with legal and regulatory developments.

10. Policy Governance

The AML Policy will be reviewed and approved by the Board of Directors at least annually. Updates may be made as necessary to reflect changes in regulations, business operations, or risk exposure.

11. Approval

This Anti-Money Laundering Policy is approved by the Board of Directors of **UNIVERSAL PAYMENT NETWORK LIMITED** and is effective as of 29th May, 2025.