

AfrimaxPay Limited Anti-Money Laundering (AML) Policy

1. Purpose and Scope

This Anti-Money Laundering (AML) policy establishes AfrimaxPay Limited's commitment to preventing money laundering and terrorist financing through its services, including the PaySimati/Paymaat e-payments service. This policy applies to all employees, officers, agents, and third-party service providers involved in AfrimaxPay's operations. The policy aims to ensure compliance with applicable laws and regulations in Malawi and to protect the integrity of the financial system.

2. Regulatory Framework

AfrimaxPay Limited will comply with all applicable laws and regulations concerning anti-money laundering in Malawi, including the Anti-Money Laundering Act and guidelines issued by the Financial Intelligence Authority (FIA) of Malawi, as well as international standards such as the Financial Action Task Force (FATF) recommendations.

3. Risk-Based Approach

AfrimaxPay shall implement a risk-based approach to AML measures:

- **Regular Risk Assessments:** Conduct ongoing risk assessments of products, services, and customer bases to identify and mitigate potential risks.
- **Enhanced Due Diligence (EDD):** Apply enhanced due diligence for higher-risk customers and transactions, ensuring thorough verification and monitoring.
- **Simplified Measures:** Implement simplified measures for demonstrably low-risk scenarios, ensuring proportionality in compliance efforts.

4. CUSTOMER DUE DILIGENCE (CDD)

4.1 Tiered KYC Procedures

AfrimaxPay shall implement a tiered Know Your Customer (KYC) system aligned with different account types and their respective transaction limits:

- **Prime, PrimeX, Go Member Accounts:** Basic KYC with essential documentation.
- **Agent Accounts:** Enhanced KYC, requiring additional documentation.
- **Merchant Accounts:** Comprehensive KYC with stringent verification steps.

4.2 Customer Identification and Verification

Obtain and verify customer identity information before establishing a business relationship or conducting transactions. Requirements include:

- **For Malawian Citizens:** Full name, identity document, physical address, village/district, contact details, occupation, source of funds, and expected income.
- **For Foreign Nationals:** Full name, nationality, passport details, Malawian address, home country address, occupation, source of funds, and residence permit.

4.3 Enhanced Due Diligence (EDD)

Apply enhanced measures for:

- High-risk customers, including Politically Exposed Persons (PEPs).
- Transactions exceeding MWK 2,500,000.

- Any suspicious transactions, regardless of amount.
- Customers frequently transacting near established limits.

4.4 Ongoing Monitoring

Conduct ongoing monitoring of customer relationships and transactions, regularly updating customer information and reassessing risk profiles.

5. TRANSACTION MONITORING AND REPORTING

5.1 Transaction Limits

Implement the following transaction limits:

- Prime, PrimeX, Go Member Accounts: Up to MWK 750,000/day.
- Agent Accounts: Up to MWK 20,000,000/day.
- Merchant Accounts: Up to MWK 100,000,000/day.

5.2 Enhanced Transaction Monitoring Systems

Develop algorithms that consider specific transaction patterns and limits for each account type, utilizing bespoke checks and controls. Implement real-time monitoring for high-value transactions, especially for Agent and Merchant accounts, and create alerts for unusual patterns.

5.3 Reporting

Report large currency transactions exceeding MWK 5,000,000 to the FIA within the timeframe guided by the Authority. File Suspicious Transaction Reports (STRs) for any suspicious activity within three working days. Report electronic funds transfers to the Authority as required, including:

- Local mobile money transfers for amounts exceeding MWK 300,000.
- Domestic and international electronic fund transfers by financial institutions.

6. Record Keeping

Maintain all CDD information, transaction records, and related documents for at least seven (7) years. Ensure records are readily accessible to competent authorities when required, with appropriate backup and recovery procedures. Compliance with data privacy regulations will be upheld during record-keeping.

7. Employee Training and Awareness

Provide regular AML training to all relevant staff members, conducted in person during recruitment and at quarterly intervals. Training programs will include case studies and practical scenarios to reinforce learning and awareness. The effectiveness of training will be assessed through feedback and knowledge assessments.

8. Internal Controls and Audit

Appoint a dedicated AML Compliance Officer to oversee the implementation of this policy. Conduct regular independent audits of the AML program to assess adherence to policies and effectiveness. A disciplinary process will be implemented for non-compliance with AML policies, ensuring accountability at all levels.

9. Specific Measures for E-Payment Services

Implement robust customer verification procedures for digital onboarding. Set transaction limits based on customer risk profiles and verification levels, ensuring they do not exceed established limits. Monitor the use of e-payment services for any unusual or suspicious activity, particularly in high-risk areas.

- Fraud Prevention Measures: Establish specific measures to prevent fraud in e-payment services, including customer education on recognizing potential fraud schemes and how to report suspicious activity.

10. Cooperation with Authorities

- Cooperate fully with the FIA, Reserve Bank of Malawi, and other relevant authorities
- Respond promptly to information requests from competent authorities

11. Compliance Officer Responsibilities

- Act on suspicious disclosures from officers and employees as soon as practicable
- Apply internal risk management procedures on disclosed suspicious transactions
- Report suspicious transactions to the Authority
- Allocate responsibilities and accountability to ensure staff duties related to identity verification are complied with
- Have access to the requisite board committee on AML/CFT compliance matters
- Carry out functions independently and free from undue influence

12. Cross-Border Declarations

- Report to the Authority any cross-border currency transfer, whether into or out of Malawi, amounting to at least USD 5,000
- Submit such reports without delay and within 12 hours

13. Risk Assessment Framework for New Products

- Develop a comprehensive risk assessment framework for new products or services before launch
- Evaluate potential money laundering and terrorist financing risks associated with new offerings
- Ensure appropriate AML measures are in place before introducing new products or expanding into new markets
- Regularly review and update the risk assessment based on the evolving financial landscape and regulatory requirements

14. Review and Updates

This AML policy will be reviewed annually or as needed to ensure its relevance and effectiveness considering changes in regulations, industry standards, or operational practices. The review process will involve key stakeholders, including representatives from product

management, finance, and software engineering departments, to gather diverse perspectives and insights.

15. Conclusion

AfrimaxPay Limited is committed to maintaining the highest standards of compliance with anti-money laundering regulations. By implementing this AML policy, the company aims to prevent financial crimes, protect its reputation, and ensure the integrity of the financial system in which it operates. All employees and associated parties are expected to adhere strictly to this policy to foster a culture of compliance and ethical conduct within the organization.

16. Policy Governance

The Compliance and Risk Manager will report directly to the CEO and maintain a dotted reporting line to the board of directors to ensure that AML compliance is prioritized at the highest levels of the organization. Regular updates will be provided to the board regarding the status of AML compliance efforts and any significant issues identified.

Updated: 21 December 2024