Anti-Money Laundering (AML), Combating Financing of Terrorism (CFT), and Countering Proliferation Financing (CPF) Position Statement

Introduction

Safaricom PLC is a leading telecommunication company in East Africa. At Safaricom, we are dedicated to combating all forms of financial crime, including money laundering, terrorism financing, proliferation financing, bribery, and corruption. To demonstrate this commitment, we have implemented a comprehensive framework for Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and Countering Proliferation Financing (CPF). Adherence to this framework is mandatory for all our employees and business partners.

Our AML/CFT/CPF policy is based on key Kenyan laws and international best practices, including:

- Proceeds of Crime and Anti-Money Laundering Act, 2009 (POCAMLA)
- National Payment System Act, 2011
- Prevention of Terrorism Act, 2012 (POTA)
- Money Remittance Regulations, 2013
- The Anti-Money Laundering and Combating of Terrorism Financing Laws (Amendment) Act of 2023
- The Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on the Prevention and Suppression of Terrorism) Regulations, 2023
- The Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Prevention and Suppression and Disruption of Proliferation Financing) Regulations, 2023
- Proceeds of Crime and Anti-Money Laundering Regulations, 2023
- The Companies (Beneficial Ownership Information) (Amendment) Regulations, 2023
- Financial Action Task Force (FATF) 40 Recommendations

Scope of the AML/CFT/CPF Framework

Safaricom has developed comprehensive AML/CFT/CPF policies and procedures to manage financial crime risks. These policies are regularly reviewed and updated to ensure they remain relevant and comply with evolving regulatory requirements and best practices. Available to all employees, these policies clearly articulate our position in the global fight against financial crime. The policies are reviewed annually or when necessary and approved by our Board of Directors.

Safaricom employs a risk-based approach to identify, assess, and manage financial crime risks proactively, allowing for the allocation of resources to systems and controls that mitigate these risks effectively.

The AML/CFT/CPF policy applies to Safaricom, its subsidiaries, branches, employees, agents, and partners involved in providing M-PESA or other financial services.

Framework Structure

The AML/CFT & CPF policy framework consists of several key pillars:

1. **Governance and Oversight**

   Safaricom's Board of Directors and executive leadership ensure that strong controls are in place to prevent financial crime. The Money Laundering Reporting Officer (MLRO) oversees compliance efforts, supported by department heads. Quarterly AML/CFT/CPF reports are submitted to the Board, confirming regulatory compliance, and keeping the Board informed on current trends in financial crime risk management.

2. **AML CFT CPF Risk Assessments**

   Safaricom's Risk Management Framework is aligned to ISO 31000 which has clearly detailed our risk rating methodology. The business-wide ML TF & PF risk assessment is in line with ML/TF & PF risk assessment standards developed by the Financial Action Task Force (FATF), and in line with Proceeds of Crime and Anti-Money Laundering Regulations.

   Safaricom PLC undertakes a risk assessment to enable it to identify, assess, understand, monitor, manage and mitigate the risks associated with money laundering, terrorism financing and proliferation financing.

   We undertake AML CFT CPF risk assessments prior to the introduction of a new partner, new product, new business practice or new technology for both new and pre-existing products, new business practice, including a new delivery mechanism, new or developing technologies for both new and pre-existing products.

3. **Customer Due Diligence Procedures**

   Safaricom conducts due diligence on all customers, agents, and partners. This includes verifying identification documents, screening against sanctions lists, and risk rating. Customer Due Diligence (CDD) is performed before entering any relationship, ensuring that customers align with Safaricom's risk appetite.

   High-risk customers, including Politically Exposed Persons (PEPs), are subjected to Enhanced Due Diligence (EDD). Senior management approval is required before onboarding high-risk customers.

4. Establishment of Ultimate Beneficial Owners

Safaricom identifies and verifies the natural persons behind a legal person and puts in place adequate measures to understand the nature of business, ownership and control structure when performing partner due diligence measures.

Safaricom may obtain, from a public register, the business partner or reliable independent sources, beneficial ownership information for all its legal entities.

5. Transaction Monitoring

Safaricom monitors transactions for suspicious activity related to money laundering, terrorism financing, or proliferation financing. Alerts are raised for high-risk activities, and exceptions are reported to senior management immediately.

Transaction monitoring involves use of automated systems coupled with Artificial Intelligence and Machine Learning Models, making use of rule-based and behavior-based monitoring. Employees identify red flags in transactions which are reported to the AML team for review. Suspicious activities are referred to the MLRO for immediate action.

Daily reviews ensure customers do not exceed M-PESA account or transaction limits of:

- Single transaction limit of KES 250,000
- Account balance limit of KES 500,000
- Daily debit limit of KES 500,000

In the very unlikely event that exceptions are noted, they are immediately escalated for resolution and reported to senior management. Cash Transaction Reports (CTRs) are submitted weekly to the Financial Reporting Centre (FRC) or transactions exceeding USD 15,000 through one or more accounts.

6. Sanctions Screening

Safaricom maintains zero tolerance to sanctions breaches. We do not engage in relationships with individuals or entities listed on sanctions list. All customers and employees are screened against sanctions lists from the United Nations Security Council Resolutions, European Union, Office of Foreign Asset Control (OFAC), His Majesty's Treasury (HMT), and local sanction lists provided by regulatory bodies. If a customer is found to be linked to sanctioned individuals or entities, their accounts are immediately frozen, and the relevant authorities are notified.

Employees must avoid facilitating transactions with sanctioned parties, either directly or indirectly, and follow the established escalation procedures when dealing with a sanctioned individual or entity. If a positive match is confirmed during sanctions screening, the account is frozen, and a Suspicious Activity Report (SAR) is submitted to the Financial Reporting Centre (FRC).

Sanctions screening is conducted both during onboarding and on an ongoing basis. As part of our risk-based approach, real-time screening is conducted on inbound and outbound international money remittance transactions by verifying the full name, date of birth, and nationality of the third party.

Additionally, adverse media screening is conducted to identify individuals who may be involved in illegal activities such as wildlife trade, human or drug trafficking, money laundering, terrorism financing, or proliferation financing.

7. Suspicious Activity Reporting (SAR)

All suspicious activities and/ or transactions are reported to the Financial Reporting Centre (FRC) within two days from when the suspicion arose. The Money Laundering Reporting Officer (MLRO) conducts a full investigation, and if the suspicion is confirmed, a formal report is submitted to the FRC as required by law.

All employees, agents, and partners are responsible for reporting suspicious activities. Failure to report such activities can result in fines or imprisonment. By staying alert to these red flags and adhering to the established escalation procedures, Safaricom ensures its commitment to identifying and reporting suspicious activities in line with its AML/CFT/CPF obligations.

8. AML/CFT/CPF Record Retention and Data Protection

Safaricom retains all customer records, transaction records and suspicious activity reports for at least seven years as prescribed by regulations. Complete and accurate records are retained and are retrievable during the relationship with the customer for seven years from the date when the relationship with the customer is terminated.

Safaricom's maintains all customer data safely and securely adhering to the guidelines in the Data Protection Act.

9. AML/CFT/CPF Audits

Safaricom regularly undertakes compliance reviews and audits to assess the effectiveness of its Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and Countering Proliferation Financing (CPF) policy, as well as the overall application of these programs across the Safaricom group.

Audit reports and findings are circulated to senior management, with follow-up actions taken to close out any issues identified and implement the recommended improvements. Safaricom's AML function also undergoes periodic independent audits, to ensure it maintains alignment with evolving regulatory, legal, and operational standards.

10. AML/CFT/CPF Training

Training programs have been implemented to ensure that all Safaricom staff, agents, and partners are fully informed about their AML/CFT/CPF responsibilities. Training is delivered through face-to-face, e-learning modules, videos, SMS and workshops.

11. Prohibited Customers

Safaricom does not engage with certain high-risk customers, including sanctioned individuals, shell companies, unregulated charities, or unlicensed businesses.

12. Penalties for Breach

Violations of the AML/CFT/CPF policy can result in disciplinary actions on staff or suspension of customer or partner accounts, depending on the severity of the breach.