GLOBAL AML

Anti Money Laundering

Millicom Global Anti Money Laundering and Counter Terrorist Financing Policy ("AML/CTF")

tigo MILLICOM

THE DIGITAL LIFESTYLE

Table of Contents

Policy Statement

Millicom International Cellular, S.A. (hereinafter referred to as "Millicom" or the "Company") offers Telecommunications Services ("Telco") and Mobile Financial Services ("MFS") in a number of jurisdictions, and recognizes that multi-national corporations such as Millicom have a role to play in preventing criminals and terrorists from abusing its business systems and processes to conduct their unlawful activities.

At Millicom, we are committed to doing business ethically so we can be a force for positive change everywhere we operate. Millicom will not engage in or assist any person or entity engaging in any activity reasonably believed to involve Money Laundering, Terrorist Financing, avoidance of disclosures to authorities, or other suspicious or criminal activity. Millicom works diligently to prevent criminals from abusing our business systems to further unlawful activities. Money Laundering (as defined below) is a global problem requiring a global approach.

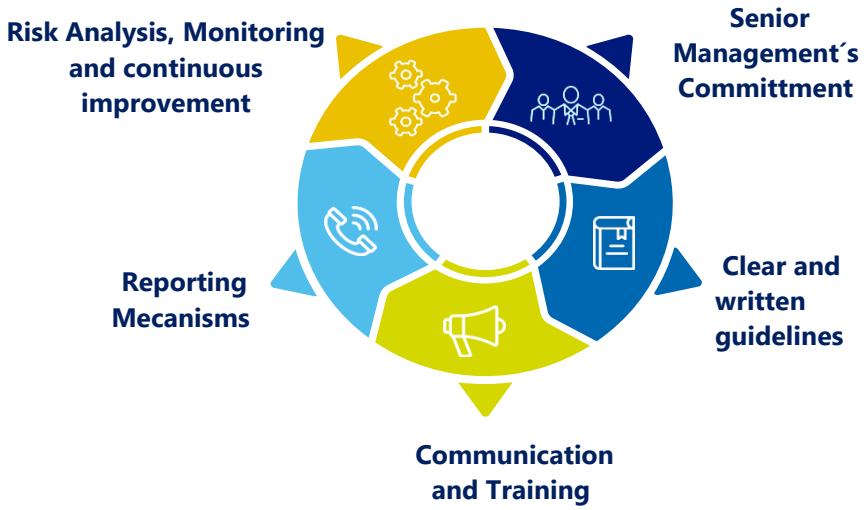
The purpose of this Policy is to reasonably address country-level AML regulatory requirements using a global standard to prevent Millicom from serving as a conduit for Money Laundering and Terrorist Financing.

Millicom is strongly committed to the highest standards of business ethics and compliance. In support of this commitment, the Company established and will enforce on an ongoing basis, policies, procedures, and standards to contain the threats of Money Laundering and Terrorist Financing in every jurisdiction in which the Millicom business operates.

This Policy applies to all Employees and management of Millicom, Tigo, Millicom group companies, as well as any Third Parties (as defined below). Where a local operation is unable to comply with this Global Policy, the Global AML Director ("GAMLD") must pre-approval in writing according to the provisions herein. This Policy should be read in combination with all other pertinent Millicom Policies.

AML Program Elements

To face the risks of the digital era, the components of the AML Program Strategy must be strengthened in the same way that the environment and its risks evolve.



Definitions

Dealer/Agent: An independent Third Party engaged by Millicom on a contractual basis to provide MFS products and services to Millicom's customer base.

Employee: Direct employees of Millicom and/or employees from all entities that Millicom owns or controls, including Directors and contracted staff.

KYC: Know Your Customer is the process Millicom uses to establish the identity of an individual or business and ensure the individual or business is not an illicit actor.

MFS: A broad range of mobile services that Millicom offers, including payments, money transfers (P2P), international remittances, savings, real-time loans, and micro-insurance.

Money Laundering: Transactions designed to evade currency reporting requirements or the source of funds (e.g., narcotics trafficking).

Suspicious Transaction: A transaction for which there are reasonable grounds to suspect that the transaction is related to a Money Laundering offense or a Terrorist Financing offense.

Telco: Telecommunications services, including residential, B2B, Pay-TV, OTT, fixed, mobile and/or wireless Internet, mobile and/or fixed telephony services.

Terrorist Financing: Illegal activities, such as drug trafficking and financial fraud, used by terrorist organizations to fund their ideological goals. Terrorist Financing includes the movement of funds through the financial system with the intention of funding terrorists or terrorist acts.

Third Party Intermediary: Any Millicom business partner, or other supplier, consultant and any other individual with whom Millicom interacts. TPI is a third party that interphases on Millicom's behalf, indirectly or directly, with government officials (such as suppliers, consultants, and other service providers).

Transaction Monitoring: The process by which customer transactions are analyzed on an ongoing basis with the purpose of detecting unusual or suspicious activities and to comply with AML and CTF laws and regulations. Transaction Monitoring will also assist AML personnel understand customer and Dealer/Agent transactional behavior.

Know Your Customer (KYC) Program

Minimum Standards. All of Millicom´s operations must establish written guidelines and procedures in place to comply with KYC procedures according to regulatory requirements. Millicom requires all customers, MFS, and Telco products and services (where applicable), including Customers, Dealers/Agents, Merchants and/or any other third party involved in a commercial agreement with both MFS and Telco operations to provide documentation of their identities. For more information on specific KYC Minimum Standards please refer to the local operation's AML / CTF Manual.

Verification of Customer Identity. The Third Party Intermediary (Dealer/Agent), or any other related party, involved in the customer onboarding process of MFS customers must capture records of customer identification and related KYC information, according to the local applicable regulatory requirements. This includes 1) Sanction Screening Process, SDNs, and Watch Lists, 2) Dealer/Agent Due Diligence, 3) Periodic Customer and Dealer/Agent KYC Review Process, and 4) Dealer/Agent Review Program ("DARP") (where Dealer/Agent are subjects to the local AML regulation). For more information on Verification of Customer Identity please see the AML / CTF Manual.

Training, Communication, and Awareness

AML training is a key component of Millicom´s Global AML program. AML training includes, but is not limited to Employees, AML Related Employees, and Dealer / Agents. Depending on the audience, the AML Training Content can include**:** definitions of key terms, practical examples of Money Laundering and Terrorist Financing activities, AML statutory requirements, and the escalation process.

The LAMLOs will develop and conduct awareness campaigns at least on an annual basis regarding AML issues, identification requirements, and related obligations to which Millicom´s operations are subject to in local jurisdictions. LAMLOs must accurately track awareness and training efforts consistent with the company's record retention requirements. For more information on Training, Communication and Awareness, please see the AML / CTF Manual.

Risk Analysis, Monitoring and Continuous Improvement

Millicom recognizes that an effective risk assessment process is essential to establishing a program that addresses AML/CTF risks. Millicom utilizes risk assessments to establish the AML program's priorities and for Millicom´s operations to deploy resources in order to comply with local regulatory recommendations / requirements, and the Financial Action Task Force ("FATF") risk-based approach.

Transaction Monitoring. All of Millicom´s operations with MFS business shall have written guidelines and procedures to ensure the ongoing monitoring of transactions to comply with regulatory requirements, the Global AML Policy, and critically, to ensure unusual activities are detected and reported to the appropriate regulatory entity. To effectively conduct transaction monitoring, each covered operation should have an appropriate , automated AML transaction monitoring system, as well as the adequate number of AML human resources necessary to conduct a meaningful investigation and documentation of the alerts raised by the system.

Reporting Suspicious Transactions. LAMLOs must report suspicious activities following local regulatory time frames. LAMLOs must keep customer and Dealer/Agent information regarding the transactional activity confidential and will not share such information with other Company departments or other parties, except when explicitly required by a competent authority.

Record Retention. Millicom keeps all records created or acquired, as required by this AML/CTF Policy or specific country regulatory requirements (including those pertaining to reporting and investigating Suspicious Transactions), in hard or electronic copy in a secure environment. The respective LAMLO shall determine which information to store and the mechanisms for their storage and retrieval in accordance with Millicom standards and local legal requirements. For more information on Risk Analysis, Monitoring and Continuous Improvement see the AML / CTF Manual

Independent AML Review

Local AML programs must be reviewed at least every twenty-four (24) months, on an annual basis if the operation's AML program is considered high risk, or more frequently if required by local regulations or changes in circumstances. A qualified independent party other than the local AML personnel, , such as an independent internal or external auditor or a regional or global AML team member(s), must conduct such reviews. Findings and recommendations resulting from independent testing will be formally communicated to the local AML team, local management team, upper management team, GAMLD, AML Committee of Millicom´s operations, and to the local Board of Directors.

Speak Up! Reporting Concerns

Employees shall immediately report violations, suspected violations, or questions regarding this Policy or any applicable law or regulation directly to a line manager, Human Resources, or any member of the Ethics & Compliance Department or report violations or suspected violations through the Millicom Ethics Line, Millicom's external and independent reporting service, which is available twenty-four hours a day, seven days a week. Contact information, country-specific numbers for Millicom's reporting service, and an online reporting mechanism are available via the Millicom Ethics Line, in the Ethics & Compliance section of the Millicom website and intranet site, , and on posters at different facilities.

Resourcing and Budgeting Plan

All of Millicom´s operations must ensure AML departments are appropriately staffed considering the size and complexity of the operation to effectively mitigate AML/CTF risks. Millicom will perform annual workload analysis to ensure increased risks or regulatory requirements align with the number of resources in the AML department.

Sanctions for Non-Compliance

Under no circumstances should a Millicom Employee violate this Policy or its related Polices. We have zero tolerance for knowingly facilitating financial crimes. Any Employee found to violate this provision will be subject to disciplinary action, up to and including termination of employment.

Resources

1.1. Code of Conduct
1.2. Anti-Corruption Policy
1.3. Conflicts of Interest Policy
1.4. Government Official Interactions Procedure
1.5. Millicom Global Investigations Manual and Procedure
1.6. Speak Up Policy
1.7. Third Party Management Policy
1.8. AML/CTF Manual

Revision History

Revision No.	Effective Date	**Changes**	**Prepared by**	**Reviewed by**
A-O	12/04/2021	Structure	Global AML Director	VP, Ethics & Compliance