GLOBAL AML

Anti Money Laundering

tigo

MILLICOM

THE DIGITAL LIFESTYLE

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

Version N° 1

Date: July 2018

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 works diligently to prevent criminals from abusing our business systems and processes 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 is hereby establishing, 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.

1. Scope of the Policy

1. This Policy applies to all Employees and management of Millicom, Tigo, Millicom group companies, as well as any Third Parties (as defined below).
    1. Where a local operation is unable to comply with this Global Policy, the Global AML Director ("GAMLD") must grant an exception in writing according to the provisions herein.
2. This AML/CTF Policy applies to Millicom business and subsidiaries, and its related Employees, Dealers/Agents, products and services within Millicom, and covers:
    - 2.1. AML Corporate Governance;
    - 2.2. AML training and awareness requirements;
    - 2.3. Know Your Customer ("KYC") policy and standards;
    - 2.4. Minimum due diligence standards for customer identification;
    - 2.5. Minimum due diligence standards for Dealer/Agent onboarding process;
    - 2.6. Monitoring and investigations;
    - 2.7. Identification and reporting of unusual or Suspicious Transactions;

2.8. Recordkeeping requirements; and

2.9. Global Policy exceptions.

3. This Policy should be read with all other pertinent Millicom Policies.

2. Who is Covered by this Policy

2.1. As previously mentioned in Section 1.1, this Policy applies to all Millicom Employees, products, and services, regardless of jurisdiction where Millicom operates, directly or through its affiliates.

3. Ownership

3.1. The GAMLD owns this Policy and is responsible for updating and amending the Policy.

3.2. Changes to this Policy require written approval of the GAMLD showing version number and effective date of the implementation and must be approved in accordance with the Millicom governance and approval process. This Policy shall be reviewed at least annually.

3.3. Where local regulations set standards lower than this Policy, this Global Policy shall apply, and it must be so stated in the local records.

4. AML/CTF Global Oversight Structure Composition

4.1. **Millicom's Board of Directors**:

1. Reviews and approves Global AML/CTF Policies and other AML-related manuals, at least annually, or when required.

2. Appoints the Executive Vice President ("EVP"), Chief Ethics & Compliance Officer.

2. **EVP, Chief Ethics & Compliance Officer**:

1. Appoints the GAMLD with an independent and sufficient authority for the oversight of AML compliance in all of Millicom´s operations.

2. Reviews and approves the Global AML/CTF Policy and its related policies, procedures, and standards.

3. GAMLD:

3.1. At the Group Level, the Employee appointed by the EVP, Chief Ethics & Compliance Officer; responsible for the oversight and administration of Millicom's AML program and this Policy for Millicom´s operations, including Telco and MFS.

3.2. The GAMLD reports to the EVP, Ethics & Compliance Officer.

4. Regional AML Program Manager (LATAM/Africa):

4.1. Employee appointed by the GAMLD; responsible for the AML oversight of respective regions, as well as Local AML Officers ("LAMLO"), and the implementation of regional initiatives.

4.2. The Company empowers regional leadership to make regional, country-specific, and local decisions necessary to assure or require compliance by the Company, Dealers/Agents, and Millicom´s Employees, in order to assure that all regional, country-specific, and local compliance requirements are addressed.

5. LAMLO:

5.1. Local Employee tasked by the corporate governance body of the local entity with the administration of the AML program and its related components, including this AML/CTF Policy.

5.2. Ensures local AML program is up-to-date and in compliance with local AML regulations and this Policy.

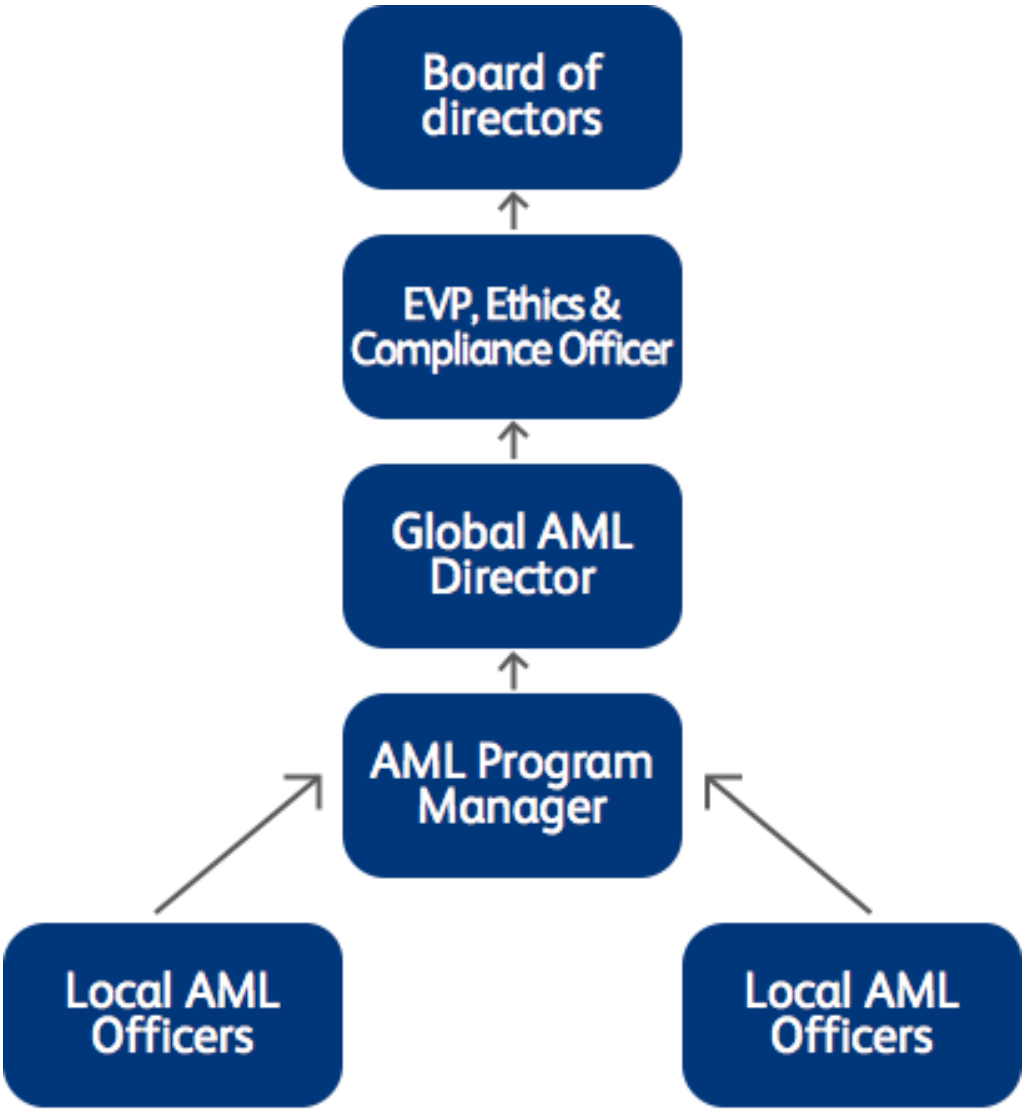
5.3. Provides AML training to applicable persons, including, but not limited to, Employees and Dealers/Agents.

5.4. Ensures Transaction Monitoring is conducted on an ongoing basis.

5.5. Reports unusual activities to the applicable regulator, as required.

5.6. Holds an independent role, reporting directly to the local Board of Directors, as required by regulation, therefore avoiding any potential conflict of interest. The LAMLOs will also report to the Regional AML Program Manager accordingly.

5.7. Approves every new product or service to be offered by MFS and communicates the decision to the GAMLD.



5.8. The Global AML organizational chart is composed as follows:

5. Definitions

5.1. **Money Laundering**: Transactions designed to evade currency reporting requirements or those involving proceeds of certain criminal activity designed to promote the criminal activity or conceal the source of funds (e.g., narcotics trafficking). Most developed nations have enacted laws aimed at detecting and preventing Money Laundering and Terrorist Financing (as defined below). The

intent of these laws is to make it difficult for criminals to use or transfer the proceeds of criminal activity.

5.2. **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. To remain "under the radar," similar to other criminals, terrorist organizations must disguise the origins of their funds to remain undetected. Terrorist organizations frequently finance their activities through legally obtained funds, such as charitable contributions.

5.3. **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. A Suspicious Transaction may include attempted transactions.

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

5.5. **AML Committee**: The management group responsible for providing overall business advice to the GAMLD. The EVP, Chief Ethics & Compliance Officer shall determine the composition of the AML Committee.

5.6. **Employee**: Direct employees of Millicom and/or employees from all entities that Millicom owns, owns a 50% stake in, or controls, including, but not limited to, members of the Board of Directors, directors, and contracted staff.

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

5.8. **KYC:** The process Millicom uses to establish the identity of an individual or business and ensure the individual or business is not an illicit actor.

5.9. **Office of Foreign Assets Control ("OFAC"):** An agency of the U.S. Department of the Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the U.S. The list of countries, organizations, and individuals subject to sanctions programs is updated in the official website maintained by the U.S. Department of the Treasury. All U.S. persons (including U.S. incorporated entities and foreign branches) must comply with applicable AML requirements.

5.10. **Specially Designated National ("SDN"):** An entity or individual who OFAC has designated as being subject to sanctions. U.S. law prohibits any U.S. person, including U.S. citizens and permanent resident aliens regardless of where they are

located, all persons and entities within the U.S., and all U.S. incorporated entities and their foreign branches from dealing with SDNs. One of the principle ways in which OFAC administers its program is through the SDN and Blocked Persons List ("SDN List").

5.11. **Third Party**: Any business partner, or other supplier, consultant, and/or any other individual with whom Millicom interacts.

5.12. **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.

6. General Principle

6.1. Millicom will not engage in or assist:

6.1.1. Any person or entity engaging in any activity reasonably believed to involve Money Laundering, Terrorist Financing, or other suspicious or criminal activity;

6.1.2. Any customer in structuring financial transactions in order to avoid disclosure to governmental or law enforcement authorities under applicable law; or

6.1.3. The disclosure of the existence or any details of an investigation or reports of Suspicious Transactions.

7. KYC Processes – Customer Identification Program

7.1. **Minimum Standards.** All of Millicom´s operations shall have written guidelines and procedures to comply with KYC procedures according to regulatory requirements. Millicom requires all customers of multiple products and services, MFS and Telco products and services (where applicable), including clients, Dealers/Agents, and any MFS and Telco personnel to provide documentation of their identities.

7.1.1. For every local operation, the respective LAMLO will determine the KYC and identification documentation required under local regulations, including, but not limited to: a valid national identity card or any other document, such as passport, or driver's license, as determined and accepted by the local laws and regulations.

7.1.2. The Company will capture the following information as part of the registration process in the pertinent KYC form or contract: (i) full name,

including surname; (ii) date of birth; and (iii) full address. The Company will capture all other information required by local regulations.

7.1.3. The Dealer/Agent shall accurately and completely record contact details, including the mobile number associated with the MFS used to open the account.

7.1.4. Customer Onboarding Process: Local business operations (MFS and Telco) shall have a written onboarding process in place that complies with local regulatory obligations.

7.2. **Verification of Customer Identity.** The Third Party (Dealer/Agent) involved in the customer onboarding process shall capture records of client identification and related KYC information, according to the Company´s local regulatory requirements. The Company will keep all relevant information for the duration of the relationship and thereafter for a minimum period of five (5) years (or longer if required by local regulations). To the extent information collected herein is not immediately available to the local corporate office, the Dealer/Agent shall transmit the records to the corporate office within a reasonable period of time, as determined by the LAMLO, or according to the time frame agreed upon in the contract, or as required by local regulations.

7.3. **Sanction Screening Process, SDNs, and Watch Lists.** All of Millicom´s operations shall screen all customers, Dealers/Agents, and Employees against watch lists on a regular basis, determined by local regulatory requirements. Millicom will report positive matches to law enforcement and/or local regulatory bodies pursuant to applicable legal requirements.

7.3.1. At a minimum, Millicom´s operations shall screen the identities of customers at the onboarding process and on an ongoing basis thereafter. These include Dealers/Agents and Employees. At a minimum, Millicom's operations will filter customers through the OFAC SDN List and any other lists required by local country regulations.

7.3.2. Human Resources must regularly check the identities of Employees against the watch lists and perform additional due diligence and background checks when required. The LAMLO must verify that the tests are timely completed and that the tests result in no positive matches. Human Resources must implement a process to deal with Employees who are positively matched to any of these lists.

7.4. **Dealer/Agent Due Diligence.** All of Millicom´s operations shall have written guidelines and procedures to verify that Dealers/Agents are reputable and will not provide the MFS or Telco, or any additional product's platform or core system to facilitate Money Laundering or Terrorist Financing. Dealers/Agents must undergo a due diligence onboarding process which each LAMLO will determine according to local regulatory requirements.

7.5 **Periodic Customer and Dealer/Agent KYC Review Process.** All of Millicom´s operations shall have written guidelines and procedures to review their customer and Dealer/Agent KYC information on an ongoing basis, utilizing a risk assessment (risk-based approach). Customer and Dealer/Agent risk ratings must be obtained from a risk assessment/matrix in accordance with Section 8.0 of this Policy.

6. **Dealer/Agent Review Program ("DARP").** All of Millicom's operations must perform oversight on their business partners, which include Dealers/Agents. Oversight includes testing the Dealer/Agent´s level of compliance with Millicom's minimum AML expectations, such as level of AML knowledge, training, unusual activity identification and reporting, and monitoring according to Millicom's Dealer/Agent Review Program Policy.

8. AML Risk Assessment/AML Risk Matrix

8.1. 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 the Financial Action Task Force ("FATF") risk-based approach.

8.2. All of Millicom´s operations shall have written guidelines and procedures to evaluate the following key risk categories in order to identify situations that could be more susceptible to Money Laundering and/or Terrorist Financing activities, and to highlight and address areas for additional risk mitigation in an efficient and effective manner.

8.2.1. Key risk categories include, but are not limited to:

8.2.1.1. Customer and Dealer/Agent risk;

8.2.1.2. Product and service risk;

8.2.1.3. Geographical location/country risk; and

8.2.1.4. Transactional behavior/consumer risk.

8.3. Each of Millicom´s operations must review its risk assessment at least annually, or when factors alter the risk of the customer or Dealer/Agent, or as required by local regulations.

8.4. This risk rating of the customer or Dealer/Agent will determine the parameters for enhanced programs and controls in the identified high risk jurisdictions and whether to implement Enhanced Due Diligence ("EDD") and additional controls. High risk customers and Dealers/Agents must undergo an EDD process at least annually, or as required by local regulations.

8.5. As new risks are identified or presented within Millicom´s operations, the LAMLOs should establish additional controls for mitigating such risks.

9. Training and Awareness

AML training is a key component of Millicom´s Global AML program. The AML training includes, but is not limited to:

1. **Employees.** All Employees, including members of the Board of Directors, must receive AML-related training.

    1.1. Millicom provides targeted initial and ongoing training on AML and this AML/CTF Policy at the time of hire for Employees.

    1.2. Employees must receive initial Employee training within thirty (30) days of hire and thereafter, as determined by the GAMLD.

    1.3. All Employees, including members of the Board of Directors, must receive AML-related refresher training at least on an annual basis.

2. **AML-Related Employees**. AML-related Employees shall receive targeted initial and ongoing training. Many members of the AML compliance leadership team are certified AML, compliance, risk, or fraud professionals who are required to complete relevant training courses to maintain their certifications.

3. **Dealers/Agents.** All of Millicom´s local operations shall provide initial and ongoing AML training to Dealers/Agents.

    3.1. Dealers/Agents must receive initial AML training within thirty (30) days of onboarding, or as determined by local regulations.

    3.2. All Dealers/Agents must receive AML-related refresher training at least on an annual basis, according to a schedule of training prepared and approved by LAMLOs.

4. **AML Training Content.** AML training must include, but is not limited to:

    4.1. Definitions of key terms;

    4.2. KYC and Dealer/Agent requirements adopted locally;

    4.3. Practical examples of Money Laundering and Terrorist Financing activities (typologies) that Employees and Dealers/Agents should be aware of;

    4.4. The AML regulatory and statutory requirements applicable in the particular jurisdiction;

    4.5. The escalation process to report suspicious or unusual activities and where to direct questions regarding this Policy or local regulatory requirements; and

4.6. Disciplinary actions for non-compliance.

5. **Training Records**

5.1. LAMLOs must appropriately record training, indicating date of the training, topic, details (including signatures) of trainees, business information, location, and specification (initial or targeted training).

5.2. LAMLOs must retain records for the required recordkeeping period according to the country's regulatory requirement. Training records should include training materials, delegate lists, date of training, and test marks. The Company retains training records for a period of five (5) years from the date of the training in hard or electronic copy in a secure environment, or longer if required by local regulations.

6. **Awareness Campaign.** The LAMLOs shall generally develop 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, with the goal of highlighting Millicom´s commitment to follow the law and assist in the fight by regulatory authorities to detect Money Laundering and Terrorist Financing.

1. Transaction Monitoring

2. All of Millicom´s operations shall have written guidelines and procedures to ensure Transaction Monitoring for complying with this Policy and with regulatory requirements.

2.1. Transaction Monitoring is an exercise that allows companies to understand customers' and Dealer/Agents' transactional behaviors, as well as to uncover unusual activities that the Company must report to local regulatory entities as required. Local operations must conduct an in-depth Transaction Monitoring exercise on an ongoing basis.

2.2. Millicom's operations must monitor transactions on an ongoing basis to identify any potential Suspicious Transactions and ascertain the likelihood of Money Laundering and/or Terrorist Financing activities taking place through Millicom platforms.

2.3. Transaction Monitoring alerts (for any monitoring system used) must at least include Millicom's recommended scenarios, including additional alarms based on local regulatory or operation requirements.

2.4. Transaction Monitoring and reporting are critical internal controls, which focus on identifying unusual activity through law enforcement or regulatory inquiries, referrals, and Transaction Monitoring system output.

11. Reporting Suspicious Transactions

11.1. 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.

1. LAMLOs must conduct periodic reviews at least on an annual basis of pre-set alarms or scenarios set-up in monitoring systems to ensure unusual activity is effectively identified, risk is mitigated, and regulatory requirements are met.

2. The GAMLD will oversee AML monitoring with the support of the LAMLO and will report on a quarterly basis to the EVP, Chief Ethics & Compliance Officer and senior management a summary of the testing conducted and the results obtained to communicate the level of risk encountered in the operation.

   2.1. The GAMLD will review the rules for generating monitoring alerts established by the LAMLOs.

   2.2. LAMLOs, under the supervisions of the GAMLD, EVP, Chief Ethics & Compliance Officer, and the respective Regional AML Program Manager, investigate alerts produced and participate in any associated case management, where applicable per local regulations.

   2.3. LAMLOs must keep all investigations of Suspicious Transactions confidential and not inform subjects of the investigations to any person other than the competent authority.

   2.4. LAMLOs must submit the required Suspicious Activity Reports ("SARs") and any other regulatory reports established in the time frame required by local regulations, (e.g., currency transaction reports or Suspicious Transaction reports).

3. The GAMLD coordinates with other internal control functions, as appropriate (e.g., Ethics & Compliance, Investigations, Internal Control, Risk, Legal, Finance, Security, Factory, Revenue Assurance) to conduct investigations, provide information where required by local regulations, and make recommendations, which are escalated to the AML Committee.

4. For more information regarding Millicom's reporting and investigation processes, please consult the Speak Up Policy and the Millicom Global Investigations Manual and Procedure.

12. Recordkeeping

12.1. **Record Retention.** Millicom keeps all records created or retained, 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.

12.2. **Five-Year Requirement.** Unless otherwise established by local regulations, this Policy requires the Company to retain records for a period of five (5) years. If applicable local regulations require a longer retention period, the regulatory period shall take precedence. The record retention process must ensure that all records are available, in a timely manner, upon request from regulatory authorities, internal audit and control functions, and external auditors.

13. Independent Review

13.1. Local AML programs must be reviewed at least every twenty-four (24) months, or on an annual basis if the operation's AML program is considered high risk after appropriate review. An independent party, such as an independent internal or external auditor, 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 Board of Directors.

14. New Product and Service AML Approval

14.1. Regulatory requirements could affect the different characteristics or requirements of Millicom's new products and/or services. AML laws and regulations could affect these requirements; therefore, it is imperative that LAMLOs are included in new products or services approval process to ensure compliance with these requirements.

15. Speak Up! Reporting Concerns

1.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.

1.1. 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 sites, and on posters in your facility's Employee posting area.

1.2. All line managers shall be responsible for the enforcement of and compliance with this Policy, including providing Employees necessary access to the latest version of this Policy.

1.3. Millicom will take disciplinary action against anyone who retaliates against Employees who initiate or participate in Ethics & Compliance Department investigations.

1.4. While Millicom encourages Employee reporting, Millicom does not tolerate false reports made simply to harm another Employee.

16. Resourcing and Budgeting Plan

16.1. 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 analyses to ensure increased risks or regulatory requirements align with the number of resources in the AML department.

17. Sanctions for Non-Compliance

17.1. Under no circumstances should a Millicom Employee violate this Policy or its related Polices. There will be 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.

18. Dispensation Process

18.1. Where local operations are unable to comply with this AML/CTF Policy, whether pursuant to local regulations or business practice, the Company will communicate its decision to the GAMLD for further action.

19. Resources

19.1. Code of Conduct

19.2. Anti-Corruption Policy

19.3. Conflicts of Interest Policy

19.4. Gifts & Hospitality Policy

19.5. Government Official Interactions Procedure

19.6. Millicom Global Investigations Manual and Procedure

19.7. Speak Up Policy

19.8. Sponsorships & Donations Policy

19.9. Third Party Management Policy

20. Revision History

Revision No.	Effective Date	**Changes**	**Prepared by**	**Reviewed by**
A-O	[insert date]			
Latest Revision Approved By:			**Signed:**	

Appendix A

Global Anti-Money Laundering and Counter Terrorist Financing Policy Certification Form

I, _____, an Employee assigned to _____ in

[Employee Full Names and Surnames] [Business]

_____, hereby certify that as of the date hereof, I have received

[Country of Operations]

a copy of the Millicom´s AML/CTF Policy, revision # _, effective _____.

[Revision #] [DD/MM/YYYY]

Further, I have read said AML/CTF Policy and have had an opportunity to ask related questions to my LAMLO.

Accordingly, I certify that I understand my personal responsibilities and obligations regarding the AML/CTF Policy and abide to comply with it.

I understand that failure to comply with the AML/CTF Policy may result in disciplinary actions, up to and including termination of employment for cause.

Signature: _____

Certification Date: _____

[DD/MM/YYYY]