

Millicom International Cellular S.A.	Policy: Fraud Management		
	Version 2	Ian Burrows	October 2017



# Fraud Management Policy

<b>File Version</b>	Version 2
<b>Last Modified on</b>	October 2017
<b>File Status</b>	Final

## Document History

Version	Date	Policy Owner	Brief Description
Version 1	September 2015		
Version 2	October 2017	Ian Burrows, Head of Business Controls	Fraud Management Policy
		<b>Executive Sponsor</b> Tim Pennington: Senior EVP, Group CFO HL Rogers: EVP, Chief Ethics and Compliance Officer	

Millicom International Cellular S.A.	Policy: Fraud Management		
	Version 2	Ian Burrows	October 2017

<b>I. TABLE OF CONTENT</b>
----------------------------

I.	Table of content.....	2
II.	Introduction.....	3
III.	Background.....	5
IV.	Fraud Management Policy.....	5
V.	Roles and Responsibilities.....	7
VI.	Annex	9

Millicom International Cellular S.A.	Policy: Fraud Management		
	Version 2	Ian Burrows	October 2017

## II. INTRODUCTION

### II.1 Introduction

This document defines Millicom’s Fraud Management Policy and is applicable to Corporate Operations and all Millicom subsidiaries, including those engaged in Mobile Financial Services (MFS) activities.

This document is complementary to and should be considered alongside relevant Millicom policies, including:

- Investigation Standard
- Revenue Assurance policy
- Whistleblowing Policy and procedures
- Millicom Code of Conduct
- Group Internal Control Manual
- Anti-Money Laundering Policy
- Anti-Corruption Policy

### II.2 Objectives

The primary objectives of this policy are:

- To promote a consistent approach to Fraud Management to ensure that malicious risks to revenues, transactions, assets (both Millicom and those held on behalf of customers, such as customer money in the MFS business), products, services, and other offerings by Millicom are identified, assessed, managed, and maintained at acceptable levels in line with Millicom’s risk appetite
- To ensure there is a consistent, clear, and concise understanding throughout all Millicom operations of the company’s zero tolerance towards fraud
- To ensure Fraud Risk Management is embedded within all Millicom business processes, in particular, the revenue life cycle, supply chain, and our MFS business
- To have all employees and outsource agents aware of the actions Millicom will take to investigate, discipline, recover assets and where appropriate take legal action in their management of fraud

### II.3 Document Owner

<b>Policy owner</b>	Ian Burrows	VP, Head of Business Controls
<b>Millicom Group stakeholders</b>	Cara Viglucci	VP, Global Investigations
	Michael Clifford	Global Investigations Manager
	Juan Ruiz	Global Investigations Manager
	Sarah Hakeem	Director, Revenue Assurance
	Linda Peralta	Global Director of Compliance
<b>Approved by</b>	Tim Pennington	Senior EVP, Group CFO
	HL Rogers	EVP, Chief Ethics and Compliance Officer
<b>Adopted by</b>	Millicom Group Audit Committee	

Millicom International Cellular S.A.	Policy: Fraud Management		
	Version 2	Ian Burrows	October 2017

#### II.4 Distribution list

Name	Title
	Group Executive Committee
	All GMs
	All CFOs
	Heads of MFS
	All Global and local Head of Departments and Managers

Millicom International Cellular S.A.	Policy: Fraud Management		
	Version 2	Ian Burrows	October 2017

### III. BACKGROUND

#### III.1 Background

Each General Manager and CFO should take ultimate responsibility to ensure that financial loss and reputational damage to the business resulting from fraud, theft, or other crime, whether internal or external, is minimised through effective prevention, detection, and investigative action. Fraud management functions in each Millicom operation should support the General Manager and the CFO in fulfilling their obligations.

Fraud Management is the responsibility of every Millicom employee, including executives, managers, staff, and outsourced staff, all of whom have an important role, particularly in the area of awareness of fraud risk and reporting concerns when they become aware of any suspect activity.

As the business environment in which Millicom operates becomes increasingly more complex, Fraud Management functions cannot mitigate all fraud risks in isolation, and will work closely with other business areas, including Product Development, Revenue Assurance, Activations, Credit and Collections, Customer Services, Retail, MFS operations and risk teams, Business/Internal Controls, Ethics & Compliance, Internal Audit and Finance functions.

### IV. FRAUD MANAGEMENT POLICY

#### IV.1 Scope and definition

'Fraud' in the context of this policy includes theft and any other intentional, malicious, or dishonest activity or omission that could result in a financial loss and/or reputational damage to any Millicom operation.

Allocation of resources to combat fraud should be based on the level of fraud risk within each Millicom operation and must be sufficient to maintain fraud losses to an agreed level. Where fraud risk is higher (for example, in Mobile Financial Services (MFS)), then additional resources should be allocated.

Total fraud losses should be assessed and reported each quarter and any remedial action evident from analysis of these losses recommended. Fraud losses are classified and reported under six main categories: Corruption, Theft, Financial statement fraud, Revenue related fraud, MFS fraud, and Procurement/supply chain fraud.

Further guidance on the fraud categories is provided in Annex VI.1.

#### IV.2 Principles

The fundamental principles in the application of this policy are:

**Legality:** Millicom, given its profile as an international group, must operate to high standards generally expected of similar organizations in Sweden, Luxembourg, the UK and U.S. All activity must meet such internationally recognized standards and comply with local legislation.

Millicom International Cellular S.A.	Policy: Fraud Management		
	Version 2	Ian Burrows	October 2017

**Proportionality:** Activity to uncover fraudulent wrongdoing and any subsequent enquiry into the individuals involved must be proportionate and considered on a case by case basis.

**Confidentiality:** Levels of confidentiality necessary and appropriate to the circumstances will be applied at all times.

### IV.3 Fraud Management Policy

It is the policy of the Board of Millicom International Cellular S.A. that each Millicom Operation maintain a zero tolerance to fraud, theft, misconduct, or other crime targeting company assets, products, or services by our employees, outsourced staff, suppliers, or other third parties.

In considering 'other significant criminal incidents' which could have an impact on the reputation of Millicom or another Millicom operation, all employees should understand the provisions and impact of their local Anti-Money Laundering and Proceeds of Crime Legislation, Anti-Bribery and Anti-Corruption Legislation along with the U.S. Foreign Corrupt Practices Act ("FCPA"), the UK Bribery Act, or similar local legislation and the impact on their operation.

Controls and deliverables required for compliance are:

- Fraud risk is periodically assessed
- Appropriate systems and processes are implemented to prevent and detect fraud, theft, and other crime. Ensure these systems are functioning and that the systems are monitored continuously or at an agreed frequency based on level or risk
- Ensure all Revenue Assurance Fraud Frameworks (IRSF, SMS, PBX, Bypass, etc.) are implemented and monitored
- All cases of insider fraud are subject of an appropriate investigation; this can be conducted by a Global or local Millicom employee, external contractor, or both
- All cases of fraud, regardless of the associated loss, are disclosed at the Operation level. This means that employees have an obligation to report fraud cases of which they are aware
- Each Millicom operation will be required to provide a quarterly fraud report using the standard reporting template provided by Group Business Controls. Additionally, the following reporting criteria apply:

Financial triggers:

- All incidents of internal fraud or third party (external) fraud, theft, or crime above \$50,000 USD, or other significant incidents are immediately reported to the Millicom Global Head of Revenue Assurance (when involving the revenue life cycle), the Global Investigations Manager, and Group Head of Business Controls
- All incidents of internal or external fraud over \$50,000 USD will be reported to the Group CFO
- All incidents of internal or external fraud over \$100,000 USD will be reported individually to the Group Audit Committee

Millicom International Cellular S.A.	Policy: Fraud Management		
	Version 2	Ian Burrows	October 2017

Non-financial triggers:

- Incidents that involve:
  - The appearance of a conflict of interest between a Millicom employee and a third party;
  - high-level management involvement in improper conduct;
  - suspicion of bribery or corruption;
  - suspicion of money laundering activity;
  - the involvement of a local/national/international official;
  - records and accounts manipulation; human trafficking, slavery, forced/child labor; and trade sanctions;
  - a significant information breach or IT security issue; or
  - the potential to seriously impact the company's reputation.

*must* be immediately reported to the Group Investigations Manager and Group VP Investigations. **If in doubt, speak up and report it.**

- All employees, outsourced staff, and suppliers must disclose any activity or suspected fraudulent activity or dishonesty to their line manager, other appropriate person, or through the confidential Millicom Ethics Line < [www.millicom.ethicspoint.com](http://www.millicom.ethicspoint.com) >

## V. ROLES AND RESPONSIBILITIES

### V.1 Roles and Responsibilities

Position	Role and responsibilities
<b>Millicom Group CFO</b>	<ul style="list-style-type: none"> <li>● Executive sponsor of the Global Fraud Policy and the Fraud Response Standard</li> </ul>
<b>Group Head of Business Controls</b>	<ul style="list-style-type: none"> <li>● Corporate owner of the Global Fraud Policy and the Fraud Response Standard</li> <li>● Responsible for fraud reporting to the Group Audit Committee</li> <li>● Responsible for Group initiatives to raise awareness of the risk of fraud and improve our ability to prevent and detect fraud across our businesses</li> </ul>

Millicom International Cellular S.A.	Policy: Fraud Management	
	Version 2	October 2017

<p><b>All Country GMs and CFOs</b></p>	<ul style="list-style-type: none"> <li>• Ensure this Policy is implemented within each operation, and compliance of said policy is to be monitored</li> <li>• Responsible for ensuring that financial loss and reputational damage to the business from fraud, whether external or internal, is minimised through effective prevention, detection and investigative action</li> <li>• Fraud risk is periodically assessed and reviewed in light of changes to the internal or external environment of Millicom</li> <li>• Ensure that incidents of fraud are reported in the manner defined in this policy</li> <li>• All employees, including outsourced staff and suppliers, must be aware that they have an obligation to disclose any activity or suspected activity of dishonesty or potential criminal acts to their manager, other appropriate person or through the Ethics Line. The ethics line is confidential and reported incidents are treated without fear of retaliation.</li> <li>• Responsible for ensuring the effective conduct of investigations in to fraud, suspected fraud and other wrongdoing</li> </ul>
<p><b>Global Investigations Manager</b></p>	<ul style="list-style-type: none"> <li>• Provide oversight of significant fraud investigations</li> <li>• Conduct investigations or reviews at the request of a GM, Global Finance function, Compliance, Legal, Corporate Security, HR or other Senior Executive</li> <li>• Provide local operations with advice and guidance on the conduct of investigations into potential incidents of fraud</li> </ul>
<p><b>Global and local Revenue Assurance Heads</b></p>	<ul style="list-style-type: none"> <li>• Responsible for the management of fraud detection and prevention systems for the end-to-end revenue cycle</li> <li>• Internal and third party (external) fraud incidents greater than \$50,000 USD as defined above should be reported to the Global Head of Revenue Assurance as well as the Group Head of Business Controls and the Global Investigations Manager</li> </ul>
<p><b>Local fraud management functions</b></p>	<ul style="list-style-type: none"> <li>• Will work closely with the heads of each department ensuring that responsibilities for malicious and benign financial risk issues are correctly allocated</li> </ul>



## VI. ANNEX

### VI.1 Fraud tree – Level 1 and level 2 fraud categories used for quarterly report

Main category (level 1)	Sub-category (level 2)
<b>Corruption</b>	Conflicts of interest (Purchasing, sales)
	Bribery, illegal payments (in cash or in kind)
	Economic extortion
	Other corruption scheme
<b>Assets misappropriation/ theft</b>	Theft of cash on hand e.g. petty cash funds
	Payroll fraud
	Expense reimbursements fraud
	Cheque fraud
	Theft of fuel
	Theft of batteries
	Theft of cell phones
	Theft of other assets
	Misuse of inventory and/or other assets
<b>Financial statement fraud</b>	Misrepresentation of books and records
<b>Revenue related fraud</b>	Subscription Fraud - To obtain handset and equipment
	Subscription Fraud - Transfer of credit
	Subscription Fraud - Services
	Subscription Fraud - Unauthorized use of data
	Subscription Fraud - SIM Swap
	Subscription Fraud - User identity theft
	Subscription Fraud - Other
	Roaming fraud
	Premium rate service fraud
	Bypass
	Wangari (missed call scheme)
	Pre pay fraud (fraudulent recharges, scratch card abuse)
	International Revenue Sharing Fraud (IRSF)
	SMS Spam
	Private Branch Exchange (PBX) fraud
	Dealer fraud (commission payment, claiming excess connections)
	Customer Service Agent Fraud (credits or discounts)
	Cable & Internet piracy
	Other Revenue related fraud
	<b>MFS (Tigo Money) fraud</b>
MFS Customer fraud	
MFS Tigo employee fraud	
Other MFS fraud	
<b>Procurement /Supply Chain fraud</b>	Bid rigging
	Supply of counterfeit/ lesser quality goods/services
	Fraudulent invoicing (overcharging, wrong products, etc.)
	Personal purchases by employees
	Other procurement fraud

Millicom International Cellular S.A.	Policy: Fraud Management		
	Version 2	Ian Burrows	October 2017

## VI.2 Detailed requirements of the Fraud Policy

### Fraud Prevention and detection

Local General Managers through their local CFOs have the primary responsibility for fraud prevention and detection in their business. In order to effectively prevent fraud, each operation must ensure processes and procedures are in place to:

- Maintain a fraud risk register of high risk fraud issues
- Periodically (at least yearly) assess and review fraud risk in light of changes to the internal and external environment at Millicom
- Undertake specialist fraud risk assessment before launching new products or initiatives
- Assess fraud risk before on boarding new customers, dealers, and agents (KYC/KYA)
- Ensure that the opportunity for fraud is reduced through the enforcement of effective management controls as specified in the Internal Control Manual such as segregation of duties, authorization of high value transactions, and management supervision
- Adherence to the Revenue Assurance Fraud Frameworks, Revenue Assurance Alarms, and Revenue Assurance General Control Frameworks
- Where applicable, work towards achieving compliance with the GSMA Mobile Money Code of Conduct
- Ensure effective controls and response by coordination of Compliance, Security, Fraud, Revenue Assurance, and Business/Internal Control departments. These arrangements must include a documented meeting at least once every two months to discuss any fraud events, develop controls, and assign responsibilities
- Conduct and document root cause analysis of every significant fraud investigation/event (including where a significant loss has been prevented) to identify control weaknesses and mitigation opportunities
- Ensure the effective implementation of mitigation measures when weakness is identified
- Share information and best practice

### Investigation and Response

In order to effectively assess, understand, and respond to fraud thereby contributing to mitigating any future loss, each operation must ensure processes and procedures are in place to:

- Ensure that every case of insider fraud is the subject of a detailed investigation carried out by a suitably experienced investigator. This may be conducted by a Millicom employee, external provider, or both.
- Ensure a report is completed in all insider fraud cases outlining the detail of the allegation, root causes, details of the investigation undertaken together with the findings, and recommendations.
- Ensure loss recovery is sought wherever possible and reported through the quarterly report to Group Business Controls.
- Ensure effective engagement with law enforcement agencies, statutory and regulatory bodies, and other key stakeholders
- Meet quarterly reporting requirements by the provision of comprehensive and accurate fraud data.
- Notify Global Head of Revenue Assurance, Group Business Controls and the Global Investigation Manager within 72 hours any fraud over \$50,000 USD (internal or external).

Millicom International Cellular S.A.	Policy: Fraud Management		
	Version 2	Ian Burrows	October 2017

- Monitor and report to local Management fraud trends identified through analysing local information, risks and vulnerabilities, e.g., number and impact of fraud cases for each main fraud category, classification of fraud cases by root cause, by identification method, etc.

## **People**

The active operational management of people is essential to an effective anti-fraud strategy. Operations must ensure the following:

- A clearly defined and documented discipline process is in place. This process should allow for independent investigation, independent adjudication, and consistently applied sanctions.
- The discipline process takes account of the Millicom zero tolerance approach to fraud and other criminal dishonesty.
- Loss recovery is pursued in all cases and particular attention is drawn to recovering losses from severance payments and bonuses. Wherever possible, this should apply where colleagues resign whilst under investigation.
- Management information on the number and outcome of disciplinary cases for fraud, theft, and other criminal activity is maintained and is available for review.
- The recruitment process should be consistent, transparent, and accountable.
- Pre-employment screening processes are to be adopted in all relevant cases (subject to compliance with local laws), with a minimum requirement of recent previous employer reference checks in all cases.
- All colleagues sign a copy of the Millicom Code of Conduct and the signed copy retained securely (on their HR personal file). Attention is drawn to section F3, and all managers should be made aware of their obligations in this regard.

## **Education and Awareness**

A critical component of a successful anti-fraud strategy is the promotion of an anti-fraud culture. In addition to the preceding guidance, operations are encouraged to:

- Ensure managers promote anti-fraud measures, demonstrate their commitment to the zero tolerance policy, and challenge suspected fraud in their relevant areas of responsibility.
- Promote and support the confidential Ethics Line in the reporting of fraud and misconduct < [www.millicom.ethicspoint.com](http://www.millicom.ethicspoint.com) >.
- Deliver anti-fraud training to all colleagues.
- Deliver anti-money laundering training to all MFS colleagues, at a minimum.
- Ensure the gifts and hospitality register is effectively utilized and supervised.
- Ensure a conflict of interest policy is in place, monitored and communicated to all colleagues.