Vodafone Ghana Mobile Financial Services Policy Standard

Anti-Money Laundering

Objective/Risk

The commitment of Vodafone Group ("Vodafone") to the highest ethical and legal standards extends to its business dealings throughout the world.

This Anti-Money Laundering (AML) Policy Standard is intended to ensure that Vodafone Ghana Mobile Financial Services (VGMFS) upholds this commitment by complying with both the specific requirements and the spirit of all relevant Ghanaian and international Anti-Money Laundering and Counter Terrorist Funding Laws, Regulations and Standards.[1] This includes compliance with the provisions of the Anti-Money Laundering Act 2008 (Act 749), the Anti-Money Laundering Amendment Act 2014 (Act 874) the Anti-Money Laundering Regulations, 2011 (L1 1987), the Anti-Terrorism Act, 2008 (Act 762), the Anti-Terrorism (Amendment Act, 2012 (Act 842) and all existing and future directives or guidelines of the Bank of Ghana on AML.

This is to avoid reputational damage to Vodafone Ghana and Vodafone Ghana Mobile Financial Services by ensuring the implementation of risk based controls that deter abuse of Vodafone Cash by money launderers and those involved in financing terrorism. It is also to protect Vodafone, its employees and third party agents from inadvertently committing money laundering and terrorist financing offences.

Policy Owner	Martison Obeng-Agyei
Policy Champion	Anita Ayivi
Day to day Contact	Naomi Hammond
Version	Version 1.3

Scope and Compliance

This Policy Standard applies to:

- All Vodafone Ghana Mobile Financial Services employees.
- All Third party partners and agents providing Vodafone mobile financial services.
- Directors, officers, employees and agents of these third party entities.

Compliance levels will be monitored on a regular basis and results reviewed by appropriate persons within the AML governance structure below. Any breach of this policy will be treated as a serious disciplinary offence and may be subject to disciplinary action in accordance with the provisions of Vodafone Ghana's disciplinary policy.

[1] In this policy all references to AML include counter-terrorist funding

Contents

1 The Policy Standard

1.1 Principles

Vodafone Ghana Mobile Financial Services shall have in place the following:

i. A Money Laundering Reporting Officer (MLRO) responsible for the day to day management of the AML compliance programme, with sufficient resources and access to all necessary customer and transaction information to carry out their duties effectively.

ii. Risk based procedures that compliment this policy as well as local regulatory requirements to be signed off by the CEO.

iii. A risk based process to verify the identity of customers as stated in section 2.1below.

iv. Due diligence on third parties conducting regulated activities on behalf of Vodafone Ghana Mobile Financial Services as stated in section 2.2

v. Transactional limits proportionate to the risk profile and level of identity verification held on the customer as stated in section 2.3

vi. Monitoring of customer and agent transactions for activity that may be linked to money laundering or the financing of terrorism as stated in section 2.4

vii. A channel for reporting suspicious customer or agent activity, both internally to the Money Laundering Reporting Officer (MLRO) and externally to relevant law enforcement bodies as stated in section 2.5

viii. Records of customer and agent transactions, identification checks, AML training and suspicious activity reports as stated in section 2.6

ix. Periodic training for all relevant employees and agents on their AML responsibilities as stated in section 2.7

x. Automated screening of all customers and owners of agencies to identify those that are sanctioned, and those that are politically exposed, and manage them appropriately as stated in section 2.8

xi. A compliance monitoring programme to assess the effectiveness of the AML controls, identify areas that require improvement and report to VGMFS Senior Management and the Group MLRO as stated in section 2.9

1.2 Definitions

Definition of acronyms and terminology:

i. **Agent** - any party in a temporary or permanent customer facing role, conducting cash-in and/or cash-out transactions, and/or registering new customers, and/or providing customer service tasks. It can include agents, aggregators, super agents, freelancers, walkers, or brand ambassadors.

ii. **Money laundering and terrorist financing** the process whereby "dirty money" produced through criminal or illegal activity is converted into "clean money" with the criminal origin very difficult to trace. E.g. a mobile financial service being used to deposit or transfer the proceeds of any crime or finance acts of terrorism.

iii. **Financial Action Task Force (FATF)** – an inter-governmental body which sets standards, and develops and promotes policies to combat money laundering and terrorist financing.

iv. **Politically Exposed Person (PEP)** – individuals, who are or have been entrusted with prominent public functions in any country, (for example Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials), their immediate family, and their close associates. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

v. **Low Risk Accounts** – domestic, on-network mobile financial services with a maximum total throughput limit of GHS 3,600 per annum.

vi. **Third Party** – any non-Vodafone entity that undertakes regulated business on behalf of Vodafone. It can include hubs, partners, Agents, or merchants.

2 Controls and deliverables required for compliance

The following are the controls and deliverables required to accomplish compliance with the principles above:

2.1 Know Your Customer

All prospective customers wishing to use Vodafone Cash must have their identity verified using reliable, independent documentary and/or electronic sources. The verification must take place prior to an account being opened or a transaction being performed with the Customer. When evidence cannot be produced, the application should be declined.

The identity checks carried out on non-face to face applicants should be designed to mitigate increased risks posed by non-face to face business e.g. identity theft.

Additional know your customer (KYC) information should be obtained on all new and, where appropriate, existing customers. KYC information includes, but is not limited to:

- Full Name
- Date of Birth
- Address
- Telephone Number
- An acceptable national ID (Passport, National ID, Voter ID card, Driver's license only).

The extent of the KYC information obtained should be determined on a risk-based approach, depending on the type of customer, level of transaction and other relevant risk factors as a minimum, a low risk customer would be required to provide full name and an ID.

For enhanced KYC, Customers in addition to the KYC requirements above will have to provide the following:

- Tenancy Agreement
- Utility Bill
- Income Tax Certificate
- Bank statements
- Reference letter or Employee's reference letter.

Customers categorised as Politically Exposed Persons should be subject to enhanced KYC checks.

For non-personal customers (e.g. agents), the KYC information should include the nature and purpose of the business, ownership and control structure. Based on this information, appropriate identification and verification checks should be carried out. The required information should include:

- Business/Corporate registration documents
- Copies of IDs of the Directors and Beneficial Owners
- TIN and Tax Certificates
- Shareholders and their nationalities.

Unregistered customers (Over the Counter Customers) who use Vodafone Cash must be required to provide identification (ID) in order to conclude the transaction and be subject to transaction limits more stringent than a registered customer.

Detailed KYC procedures shall be contained within the **Vodafone Ghana AML Procedures Manual** taking into account Ghanaian legal or regulatory requirements.

2.2 Third Party Management

Robust and effective controls must be in place for all third parties that undertake regulated business on behalf of Vodafone Ghana Mobile Financial Services, for example, agents who register and conduct transactions for Vodafone Cash. Appropriate due diligence must be conducted prior to business commencing. This will include, but is not limited to, verification of the nature and purpose of the business, and risk based identity checks and watch-list screening of owners and directors.

Third parties will also be formally required to adhere to AML policies and procedures, be monitored to ensure adherence, and face sanctions for breaches. Due diligence will be refreshed annually.

2.3 Systemic Transaction, Balance and Account Limits

All Vodafone Cash transactions shall have appropriate, system-enforced, transaction amount /volume and balance limits in place across all account and customer types, taking a documented risk based approach proportionate with the level of KYC. This requirement applies equally to unregistered customer transactions. The objective of these limits is to proactively deter the use of the service in channelling of proceeds of crime.

The maximum transaction throughput per customer/agent should be proportionate with the level of KYC and as provided under the provisions of the Bank of Ghana Guidelines for E-Money Issuers in Ghana or its relevant amendments from time to time. The MLRO and Policy Owner must sign-off on transaction limits in place for mobile financial service products

2.4 Transaction Monitoring

In order to identify potential suspicious activity, monitoring of transactions and account activity should be carried out using a documented risk based approach.

Transactions and account activity of customers categorised as Politically Exposed Persons should be subject to enhanced monitoring.

2.5 Suspicious Activity Reporting

The Vodafone Ghana Money Laundering Reporting Officer (MLRO) is responsible for the receipt, investigation and disclosure (where appropriate) of suspicious activity reports from employees and third party agents as directed under the Bank of Ghana Guidelines for E-Money Issuers in Ghana.

The AML procedure manual shall contain procedures for employees to report suspicions of money laundering to the MLRO for further investigation.

The MLRO shall then conduct a full investigation into the suspect's activity including a review of any connected accounts, businesses or agents. If the suspicion is validated, a report shall be submitted to the Financial Intelligence Centre as required under Act 749 and any other relevant legislation of Ghana.

Information about a suspicious activity report made internally to the MLRO or externally to the authorities must not be disclosed to customers.

When a customer has been subject of a suspicious activity report validated by the MLRO, a decision should be made as to whether the account(s) should be closed. This decision should be made by the MLRO and senior management, taking into account risks applicable to Ghanaian legislation such as tipping off the customer that a suspicion exists by closing the account with no logical explanation.

2.6 Record Retention

A record of all registered customer and agent KYC information (ID records and transaction history) must be kept for a **minimum of 6 years** after the relationship with Vodafone (or partner) has ended. This includes any copies taken of documentary evidence of identification and residential address verification.

Exception: Customers who are categorised as low risk and therefore qualify for simplified due diligence do not require a copy of identification. However, a reference number that would enable the document to be reproduced must be stored.

Transaction records must enable the transaction to be reproduced and therefore include the amount, names, (example of originator and beneficiary of a Vodafone Cash transaction) and the currency.

Records of suspicious activity reports made internally to the MLRO and externally to the authorities must be kept for a **minimum of 6 years** after the report is made. This should include details of the investigation carried out and the logic behind the MLRO's decision.

All of the above mentioned records must be stored securely and be easily accessible to the MLRO.

At the end of the six (6) year period, the records shall be sent to the Public Records and Archives Administration Department in accordance with Act 749 of Ghana.

2.7 Employee and Agent Training

All new employees (including temporary, contract and agent employees) and Agents whose roles involve working with the Vodafone Ghana Mobile Financial Services must complete induction training in relation to their roles within 30 days of their start date (or prior to commencing for Agents) and refresher training at least once every year from a competent trainer. This will be general AML awareness training tailored to Ghanaian AML legislation and risks associated with the products and services offered. Employees are required to demonstrate awareness by passing a knowledge test.

Employees in higher risk or key programme areas must complete more detailed training covering money laundering risks specific to their area. The minimum frequency for this training will be once every year.

The MLRO is required to complete specialist AML training in the form of a recognised qualification.

On-going records of all AML training must be securely maintained and kept for 6 years after an individual has left Vodafone's employment.

2.8 Watch-List Screening

Accounts must not be opened and services not provided for sanctioned individuals and any existing accounts identified in the name of sanctioned individuals must be immediately closed and the relevant authorities notified.

All applicants (individuals and entities) should be screened against relevant sanction lists, namely:

- United Nations
- European Union
- Office of Foreign Asset Control (OFAC), US
- HM Treasury, UK
- US Sanctions List
- Any other list as required under the Anti-Money Laundering Act, 2008 of Ghana (Act 749).

All existing customers should be screened against the above lists periodically (at least annually), and records maintained of this action.

Customer and agent accounts applied for by individuals meeting the definition of a Politically Exposed Person (PEP) must be subject to approval from VGMFS Senior Management Team. Approved accounts held by PEPs require enhanced KYC checks and transaction monitoring, and should be logged on a central database.

2.9 Compliance Monitoring

Adherence to this policy as well as its related procedures shall be monitored by the Vodafone Ghana Mobile Financial Services' MLRO. Compliance breaches will be reported to both VGMFS Senior Management Team and the Group MLRO and local regulator where appropriate.

A documented Compliance Monitoring programme will exist to regularly assess compliance with AML Policy and procedures and the effectiveness of the AML controls, identify areas that require improvement.

The findings and analysis of monitoring (including breaches and areas requiring improvement) will be reported to both the local senior management and the Group MLRO. This must include documented reporting to local Exco Policy Owner and local Compliance Committee or equivalent.

Local procedures must include random sample checking of data, and on-site and off-site agent monitoring.

An annual MLRO report will be submitted to Vodafone Ghana Mobile Financial Services' governance body and the Group MLRO, outlining VGMFS's AML compliance status. This report will feed into the Group MLRO annual report outlining compliance levels and any areas that require strengthening.

Regular compliance reviews would be carried by local internal and nominated external auditors.

3 Off-Network Transactions

Off-network transactions are any which leave the internal financial ecosystem. This includes International Money Transfers and Interoperable Transfers. These types of transactions are higher-risk than internal transfers as control and visibility moves to a Third Party. To ensure that these risks are effectively mitigated, robust and tailored controls must be implemented prior to the commencement of off-network transactions.

Eligibility to use these services must be restricted to customers who have been able to complete the Standard KYC process at a minimum.

Appropriate controls including targeted systematic transaction monitoring, partner due diligence and documentation of processes between internal and third party AML teams are also required. System capabilities must also be in place to comply with FATF Recommendation 16 on wire transfers and provide information on the payer and payee accompanying the transfer of funds.

The MLRO must discuss AML requirements with the Group MLRO prior to any off-network service being offered, to ensure that all requirements are implemented.

4 Roles and Responsibilities

The **CEO** of Vodafone Ghana Mobile Financial Services through the Head of Legal has ultimate responsibility for compliance to this Policy Standard, the Anti- Money Laundering Act, 2008 Act 749) of Ghana, the Bank of Ghana's Guidelines on AML and any other relevant Ghanaian legislation.

The **MLRO** will be formally appointed by the CEO. Further to their role of reporting suspicious activity to the local authorities, the MLRO will be responsible for ensuring that Vodafone Ghana Mobile Financial Services conforms to this Policy Standard as well as all local legislation. The MLRO will ensure processes are in place to meet this Policy Standard.

The **Group MLRO** will oversee compliance across Vodafone Group and support the local markets including Vodafone Ghana Mobile Financial Services in the implementation of the AML programme.

5 Exceptions

Exceptions may be permitted in cases where relevant legislation of Ghana conflict with this Policy Standard. The Group MLRO must be informed in writing in such instances. All other exceptions are subject to prior written approval from Group MLRO

6 Supporting Documents

Where Ghanaian laws and regulations require lower levels of compliance than Vodafone Global Policy, Vodafone Ghana Mobile Financial Services will in addition to the local standards, apply the Vodafone Global Policy Standard except where provisions of such policy standard conflict with relevant legislation of Ghana in which case the laws of Ghana will prevail.

7 Document History

Version	Date	Changes	Other standards affected	Approved by
1	14 June 2016	Original document	VF Ghana – Anti-Money Laundering Policy Standards VF Ghana – AML Procedures Manual	Theodore Albright
1.1	17 October 2016	Updated to reflect new group AML policy	VF Ghana – AML Procedures Manual	Theodore Albright
1.2	21 December 2016	Amended to reflect changes in the law (i.e. regulatory requirements)	VF Ghana – AML Procedures Manual	Theodore Albright
1.3	10 April 2018	Amended to reflect new Policy owner and Champion	VF Ghana – AML Procedure Manual	Martison Obeng-Agyei