FINANCIAL INTELLIGENCE UNIT, SIERRA LEONE

# DIRECTIVES & GUIDELINES FOR MOBILE MONEY SERVICE PROVIDERS ON THE PREVENTION OF MONEY LAUNDERING & TERRORISM FINANCING

ISSUED BY
THE FINANCIAL INTELLIGENCE UNIT

*Help the Financial Intelligence Unit combat dirty money*

Table of Contents

## INTERPRETATION

Except otherwise expressly provided the following words and expressions shall have the meaning attached to them:

**"Agent" means:** a natural or legal person that provides agency services to customers on behalf of a principal under an agency agreement. It may serve customers at one or multiple agent points and may be under contract with theprincipal directly or with a master-agent which is in turn under contract with the principal;

**"Agent Network Manager" means:** A person that provides support services relating to the management and supervision of others who are Agents of the principal but not Agents of the network manager;

**"AML"** means Anti Money Laundering;

**"Authentication"** means the process of validating the claimed identity of the user. Therefore, authentication tools and methods shall be adopted by mobile money issuers to authenticate the users and agents of its mobile money system.

**"Central Bank"** means Bank of Sierra Leone;

**"CFT"** means Combating of Financing of Terrorism;

**"CTR"** Currency Transaction Report;

**"Data confidentiality"** means the assurance that sensitive information remains private and not able to be viewed or used by those unauthorised to do so and hence confidential data shall be maintained in a secured manner and protected from unauthorised viewing or modification during transmission and storage;

**"FIU"** means Financial Intelligence Unit;

**"FTR"** means Foreign Transaction Report;

**"Master Agent" means:** A person that is both agent and principal, that engages Agents

who are sub-agents of the Master agent's principal and act onbehalf of the Master Agent's principal;

**"Microform"** any forms of documents for transmission, storage, reading, and printing. Microform images are commonly reduced to about one twenty-fifth of the original document size;

**"Mobile Money Operator"** means any entity that is responsible for the payment obligation and assumes the liabilities for mobile money issued;

**"Mobile money"** means a payment instrument, whether tangible or intangible that stores funds electronically in exchange for funds paid to the issuer and is able to be used as a means of undertaking payment to any person other than the issuer;

**"Mobile Network Operator"** means a mobile phone company licensed by the National Communications Authority;

**"Mobile Money Service Provider"** means an entity licensed by the Central Bank to issue Mobile Money and provide Mobile Money Services;

**"Mobile Money Services"** means services provided by the mobile money service providers to support the utility of Mobile Money for the consumer. These include but are not limited to cash in, cash redemption at various channels and mobile payments services such as person to person, business to person and government to person;

**"NatCA"** means National Communications Authority;

**"Non-repudiation"** means a process of ensuring that electronic messages are not being repudiated by its sender or receiver;

**"Operational risk" means** a risk that hardware and software problems, or human error, or malicious attack will cause a system to break down or malfunction giving rise to financial exposures and possible losses;

**"Origin"** a place where business/transaction begins or occurs;

**"Source of transferred funds"** origin of an individual's funds upon the commencement of a business/transaction;

**"Outsourcing risk"** ***means*** a risk introduced by subcontracting or outsourcing certain services or operations;

**"Politically Exposed Person"** means persons holding prominent public positions domestically or in a foreign country such as heads of state or government, senior politicians on the national level, senior government, judicial, military or party officials on the national level, or senior executives of state-owned enterprises of national importance, or individuals or undertakings identified as having close family ties or personal or business connection to such persons;

**"Reporting Entity"** means any person or entity including a financial institution who conducts as a business, for or on behalf of a customer, one or more of the activities or operations specified in parts I and II of the First Schedule of the AML/CFT Act 2012 and any other activity specified by FIU;

**"Supervisory Authority"** means the Central Bank of Sierra Leone or any other authority having oversight over a reporting entity;

**"Suspicious Transaction" means a** transaction that does not conform to the knowledge of the system operator about its customer, or a transaction is suspected to be used to commit a money laundering, terrorist financing offence or any unlawful activity;

**"Security risk"** means *a* risk where the integrity of the system becomes compromised such that it becomes vulnerable to fraud and counterfeiting*;*

**"System and data integrity"** means the accuracy, reliability and completeness of information processed, stored or transmitted;

**"Trust Account"** means a bank account which holds funds that are received from Mobile Money customers, which account is held in trust or held in a fiduciary capacity on behalf of the Mobile Money customers. This may also be referred to as an Escrow Account, a Custodial Account, or a dedicated account in a supervised bank, which holds e-money balances*;*

**"The Act"** means the Anti-money Laundering and Combating of Financing of terrorism Act 2012, Act No 2 of 2012 (as amended);

**"User"** means any person to whom the mobile money has been issued or any person who uses mobile money to make payments for purchases of goods and services;

"**The Non-Bank led Model**" This model allows a corporate organization that has been duly licensed by the Central Bank to deliver mobile money services to customers. The Lead Initiator shall be a corporate organization other than a bank or a telecommunication company specifically licensed by Central Bank to provide mobile money services. Following this model the payment transactions occur entirely within the Mobile Network operator's network, and do not require the subscriber to have a bank account. The funds in transit paid in by the remitter but not yet withdrawn by the recipient, are in principle on deposit in a separate trust account with one or more banks and are therefore not deposits in the context of banking business. Mobile network operators make use of the banking facilities, in the form of trust accounts.

The Mobile network operator only executes client payment instructions and does not perform the credit assessment and a bank's risk management role. The Mobile network operator model of mobile financial services is different from the mobile banking model in three significant aspects:

(i) Cash exchanged for electronic value are not repaid and remains in control of the customer at all times.

(ii) To offer Mobile Money Financial services, the agent must deposit a float of cash upfront in a trust account, held by a local bank. As such there is no credit risk to either the customer or the mobile network operator.

(iii) Customer funds are not on-lent in the pursuit of other business or interest income. All funds are to be maintained in a pooled trust account at a reputable bank, and cannot be accessed by the mobile network operator to fund its business. Hence, there is no intermediation, which is a key part of the deposit taking definition.

No interest is paid on customer deposits, or received by the mobile network operator on the float. This is a further factor which indicates that the e-value created is not in fact a deposit.

"**The Mobile Money ecosystem**" means various stakeholders that include the Mobile Money customer, service providers and multiple regulators including but not limited to: -

(i) "**The Mobile Money customer**" – This is a person / entity which opens a Mobile Money wallet otherwise referred to as a Mobile Money account, interchangeably, and is identified as the account holder of the Mobile Money account. The customer is in control of the Mobile Money wallet and performs transactions in the wallet.

(ii) "**The Mobile Money Agents**" These are generally informal and formal service points where Mobile Money customers are able to access Mobile Money services such as cash in; cash out and pay for goods and services. Agents do not have a direct contractual relationship with the Mobile Money customer. In most jurisdictions, the success of Mobile Money depends on non - traditional agent network for the distribution and provision of services. In this regard, agents are defined as third party entities or persons that are appointed as agents by the Mobile Money Service Provider to provide Mobile Money services on behalf of the mobile money service provider;

(iii) "**The Mobile Money Service Provider**"- This is the entity that issues Mobile Money, provides Mobile Money Services and is normally licensed by the Bank of Sierra Leone;

(iv) "**The Bank**" This provides the regulated banking facilities where the money collected by the mobile money service provider is deposited, on behalf of the mobile money customers. Mobile Money customer funds are held in the "Trust Account". In this regard, the bank is a sponsor to the Mobile Money Services Provider. The bank does not have a direct contractual relationship with the Mobile Money customer. The direct relationship is between the Customer and

the Mobile Money services provider. In most circumstances the bank is a direct participant in clearing and settlement, accordingly it clears and settles the payment obligations of the mobile money service provider;

(v) **"The Regulators"** These include the Bank of Sierra Leone, the National Telecommunication Commission and Financial Intelligence Unit, Sierra Leone.

## INTRODUCTION

These directives and guidelines address business rules governing the operation of mobile money services, specify the functionalities expected of any mobile payment services and solutions in Sierra Leone. It also identifies various stakeholders and defines their roles and responsibilities in providing mobile money services. In addition, it sets the basis for the regulation of services offered at different levels and by different service providers.

The Directives and Guidelines have identified one model for the implementation of mobile money services namely, Non-Bank Led model, or corporate organisation duly licensed by the Bank of Sierra Leone as Lead Initiator.

## 1.00. THE LEGAL AUTHORISATION TO ISSUE THESE DIRECTIVES

These Directives and Guidelines are issued under powers conferred on the Financial Intelligence Unit (hereinafter referred to as the Unit) by Section 13 (1) (J) and 133(1) of the Anti-Money Laundering and Combating of Financing of Terrorism Act 2012 (as amended 2019).

## 2.00. OBJECTIVES OF THE DIRECTIVES

**2.01**. Promote prudent and effective mobile money services in compliance with the provisions of Anti-Money Laundering and Combating of Financing of Terrorism Act of 2012.

**2.02**. Enhance customer confidence in mobile money services.

**2.03**. Provide minimum technical and business requirements for customers in mobile money services in compliance with applicable laws, regulations, directives and guidelines in force.

**2.04**. Strengthen national and sectoral effort for regulations and orderly development of mobile money services, with precise definition of various stakeholders and their expected roles and responsibilities.

## 3.00. SCOPE OF THE DIRECTIVES

These Directives and Guidelines shall apply to non-bank led mobile payments including agents, service providers and customers.

## 4.00. THE OBLIGATION TO KEEP RECORDS OF TRANSACTIONS

**4.01**. Every mobile money service provider shall keep complete accurate and reliable records sufficient to allow the reconstruction of each transaction giving details of the personal identity of the customer and related information including but not limited to the name of the customer, address of customer, place of work of customer, designation of customer, nationality of customer, date and place of birth of customer, national identity card, passport, driver's license or voter identity card and any other or further particulars that will facilitate the comprehensive identification and profiling of the customer.

**4.02**. Without prejudice to ***para 4.01*** every mobile money service provider shall clearly identify any beneficial owner different from the customer directly dealing with mobile money service provider in the mode prescribed thereby.

**4.03**. Every mobile money service provider in compiling the records of a transaction in compliance with ***para 4.01 and 4.02*** shall clearly indicate transaction details including but not limited to the nature and date of the transaction, type and amount of currency involved, type and identifying number of any account used or quoted in the transaction with sufficient identification of the holders thereof and any further particulars that would facilitate the reconstruction of the transaction.

**4.04**. Where a transaction involves securities and investment, the mobile money service provider in compiling transaction records in compliance with ***para 4.01 and 4.02*** shall

include details of the security and investment subject of the transaction including but not limited to the following:

(a) The nature of such securities/investments;

(b) valuation/s and price(s);

(c) Memoranda of purchase and sale;

(d) Sources and value of funds and bearer securities;

(e) Destination of funds and bearer securities;

(f) Book entries;

(g) Custody of title documentation;

(h) The nature of the transaction;

(i) The date of the transaction;

(j) The form (e.g., cash, cheque) in which funds are offered and paid out;

(k) The type and amount of currency involved;

(l) The type and identifying number of any account involved in the transaction;

(m) Account files and business correspondence;

(n) Any further particulars that would facilitate the reconstruction of the transaction and analysis thereof

**4.05**. Without prejudice to ***para 4.1, 4.02, 4.03 and 4.04***, in dealing with transactions involving electronic transfers, every mobile money service provider shall retain records of payments made with sufficient details to enable them to establish data including but not limited to the following:

(a) The identity of the remitting customer;

(b) Origin and source of transferred funds;

(c)The identity of the ultimate recipient;

(e)The form of instruction and authority;

(f) Destination of the funds and

(g) Any further or other particulars that would enable the reconstruction and analysis of the transaction.

**4.06**. Where a transaction involves domestic or international credit transfer made by electronic means the mobile money service provider shall include as part of their records the particulars of both the ordering and beneficial customers including but not limited to

their names and addresses, their account numbers and any other particulars that would facilitate the accurate and reliable identification and verification of the customer and the reconstruction of the transaction.

**4.07**. Every mobile money service provider shall ensure that all sets of data collected and maintained in compliance with ***para 4.01, 4.02, 4.03, 4.04, 4.05 and 4.06*** of these directives are kept in a readily retrievable and accessible form without prejudice to the confidentiality obligation as provided for by the Act

**4.08**. Every mobile money service provider shall ensure that the records and data contemplated hereby are kept and secured in any retrievable form including but not limited to the following:

(a) An original hard copy;

(b) Microform;

(c) Electronic data; or

(d) Any other form that would ensure the security and easy accessibility of the data

**4.09**. For the purposes of ***para 4.08***, records held by third parties shall not be regarded as being in a readily accessible and retrievable form unless the mobile money service provider is reasonably satisfied that the third party is an institution able and willing to keep such records and disclose them in a timely manner to the mobile money service provider when required.

**4.10**. Every mobile money service provider shall ensure that all records and data kept and, maintained under ***para 4.01, 4.02, 4.03, 4.04, 4.05, 4.06, and 4.07*** are preserved for a period not less than 5 years following the end of business relationship.

**4.11**. It shall be mandatory for any mobile money service provider to forward any record or data kept and maintained under these directives to FIU, and the Bank of Sierra Leone upon request.

## 5.00. MOBILE PAYMENTS PROCESSES

**5.01**. Every mobile money service provider shall put in place measures that covers the entire solution delivery, from customer registration and management, agent recruitment and management, consumer protection, dispute resolution procedures, risk management processes, to transaction settlement as provided by the mobile payment ecosystem.

**5.02**. All processes contemplated by ***para 5.01*** shall be implemented in compliance with the provisions of the Anti-Money Laundering and Combating of Financing of Terrorism Act of 2012 and any other laws, regulations, directives and guidelines in force.

## 6.00. KNOW YOUR CUSTOMER (KYC) AND CUSTOMER DUE DILIGENCE (CDD) REQUIREMENTS

**6.01**. Every mobile money service provider (MMSP) shall verify customers in accordance with section 20 of the Anti-Money Laundering and Combating of Financing of Terrorism preventive measures so that criminals will not misuse the mobile money payment systems, products or any facilities offered for the purposes of money laundering, terrorism financing, proliferation financing, and predicate offences.

**6.02**. An approach in the implementation of KYC and CDD is required to pave the way for a successful financial inclusion strategy of mobile money services following the directives on Tiered Know Your Customer (KYC) June 2020.

**6.03**. Organizations processing bulk payments shall be subjected to the limits imposed in ***para 6.02*** as provided without prejudice for transactions processed by every organization and shall abide by the stipulated transaction limits.

**6.04**. Every mobile money service provider shall put in place adequate risk management systems to determine whether a potential or existing customer or a beneficial owner or principal in a relationship or transaction is a politically exposed person and shall apply enhanced due diligence as stipulated by section 27 of the Anti-Money Laundering and

Combating of Financing of Terrorism Act of 2012 and any other laws, regulations, directives and guidelines in force.

## 7. 00. ROLE OF THE COMPLIANCE OFFICER

The role of compliance officers shall be clearly defined and documented in line with section 35 of the Anti-Money Laundering and Combating of Financing of Terrorism Act 2012 (as amended) as follows: -

a) be responsible for establishing and maintaining such manual of compliance procedures in relation to its business as the supervisory authority or FIU may from time to time require.
b) be responsible for ensuring compliance by staff of the reporting entity with this Act and any other enactment relating to money laundering or financing of terrorism and the provisions of any manual of compliance procedures established under this section.
c) act as the liaison between the reporting entity, the supervisory authority and FIU in matters relating to compliance with this Act and any other enactment or directive with respect to money laundering or financing of terrorism and proliferation financing.
d) establish and maintain procedures and systems to implement the customer identification requirements, implement record keeping and retention and implement the reporting requirements.
e) make its officers and employees aware of the enactments relating to money laundering, financing of terrorism and proliferation financing.
f) make its officers and employees aware of the procedures, policies and audit systems adopted by it to deter money laundering and financing of terrorism and proliferation financing.
g) screen persons before hiring them as employees; and train its officers, employees and agents to recognize suspicious transactions,

trends in money laundering and financing of terrorism and proliferation financing activities and money laundering and financing of terrorism risks within the reporting entity's products, services and operations; and establish an audit function to test its anti-money laundering, financing of terrorism and proliferation financing procedures and systems.

h) The compliance officer shall have ready access to all books, records and employees of the reporting entity necessary to fulfil his responsibilities.

## 8.00. DUTY TO ENSURE THAT ADEQUATE RISK MANAGEMENT IS IN PLACE

**8.01**. Every mobile money service provider shall establish an adequate risk management infrastructure and processes in compliance with Anti-Money Laundering and Combating of Financing of Terrorism regime taking into cognizance risk of money laundering, terrorism financing and any other unlawful activity posed by mobile money operations.

**8.02**. Every mobile money Service Provider should ensure that its systems and services maintain adequate security and internal controls to ensure the safety and integrity of the mobile money data and records, effective fraud detection and resolution mechanism, together with effective risk management arrangements.

**8.03**. It shall be the responsibility of every mobile money service provider to ensure a robust and well-tested contingency arrangement be put in place to address operational risks.

**8.04**. Every mobile money service provider shall implement operational and security safeguards that are commensurate to the scale and complexity of their schemes.

## 9.00. THE DUTY TO TAKE A RISK-BASED APPROACH

**9.01**. Mobile Money Service Provider shall in their internal control policy formulation and implementation in compliance with the Anti-Money Laundering and Combating of

Financing of Terrorism regime in force take into cognisance the risk of money laundering and terrorist financing posed by the various customers, products, services, clients, transactions, geographical factors etc, so that any Anti-Money Laundering and Combating of Financing of Terrorism measures adopted will be proportionate to the level of risk posed by a particular customer, product, service, client, transaction or geographical factor involved.

**9.02** Mobile Money Service Provider shall conduct periodic reviews (once every 1year for high risk, 3years for medium risk and 5years for low risk) to determine whether any adjustment should be made to the risk rating and ensure that the review of the risk rating for high-risk customers must be undertaken more frequently than for other customers. All decisions regarding high-risk relationships and the basis for these decisions shall be documented.

**9.03**. Mobile Money Service Provider shall pay special attention to the Know Your Customer (KYC) regime when entering business relationship with a customer, hence Mobile Money Service Provider must determine the level of risk posed by the customer before a decision is taken on whether to commence a relationship so that any Anti-Money Laundering and Combating of Financing of Terrorism measures adopted would be effective enough to counter any possible threat that may be posed by the potential customer.

**9.04**. Every Mobile Money Service Provider shall observe enhanced due diligence for higher risk categories of customers, business relationship or transaction including but not limited to:

**a)** Non-resident customers;

**b)** Private banking;

**c)** Legal persons or arrangements such as trusts that are personal asset holders;

**d)** Customers from high-risk countries and regions;

e) Politically Exposed persons (PEPs); and

f) Customers involved in money transmission and currency exchange.

9.05. Where a transaction involves the transmission of money from one jurisdiction to another the Mobile Money Service Provider involved shall document the number of underlying transactions of each transfer made to or through them by their customers so that the Mobile Money Service Provider be certain that the number and average value of transactions is consistent with the level of business disclosed by the customer to the Mobile Money Service Provider preparatory to the commencement of the business relationship and ensure that the behaviour of the client is carefully scrutinised in order to enable the Mobile Money Service Provider to report any suspicion that the transaction may be connected in whatever way with money laundering or terrorism financing to FIU without delay but not later than 48 hours. Such suspicious transactions account/number shall be blocked immediately upon reporting.

9.06. Where the customer is a money transmission or a foreign exchange business the Mobile Money Service Provider shall ensure that the proprietors or managers have followed all the due processes and procedures including but not limited to holding a license issued by the Bank of Sierra Leone before engaging in any transaction.

9.07. Where a currency exchange or transmission business customer operates within high risk jurisdictions such as a financial corridor the Mobile Money Service Provider shall carry out enhanced due diligence not only on the transaction itself but also the countries where the recipients or beneficiaries are based and take further measures to ascertain the purpose for which the funds are to be transmitted by reference to recognised Mobile Money Service Provider or other governmental and non-governmental agencies having bio-data and other records of individuals to verify any information that would have been supplied by the customer for the purpose of the transaction.

**9.08**. Mobile Money Service Provider shall pay particular attention to transactions involving the transmission of funds to high-risk countries or regions especially when:

**a)** The transactions involve large sums of money; and

**b)** The funds are designated as being transmitted for charitable purpose.

**9.09**. Where the transaction involves a charitable organisation, or the funds thereof are intended for charitable purposes the Mobile Money Service Provider shall carry out enhanced due diligence to ensure that the charitable venture is not used as a front to launder proceeds of crime or otherwise legitimate income is not used to fund terrorism or any unlawful activity behind the veil of charity.

**9.10**. A Mobile Money Service Provider carrying out or facilitating a transaction/business relationship involving charity or funds of which are intended for charitable purposes shall carry out the relevant identification verification exercise to ensure that:

**a)** Any charitable organisation contemplated by ***para 9.09*** is in existence by soliciting details of the name of the organisation, the address, the organisation's working document (if any);

**b)** Those behind the formation of the charitable organisation are identified and verified, to ensure that they have never been involved in any act or conduct connected in any way whatsoever with money laundering, terrorism financing or any unlawful activity;

**c)** The charitable organisation is legitimate under the laws of Sierra Leone by way of having gone through the various processes, protocols and procedures with all the formal documentary requirements complied with; and

**d)** The charitable organisation has the necessary financial data as required by law with the most recent audited financial reports to be made available to the Mobile Money Service Provider for the purpose of verification and authentication.

**9.11**. If the verification and identification exercise carried out under ***paras 9.09 and 9.10*** reveals suspicious circumstances in relation to money laundering, financing of terrorism, or any unlawful activity the Mobile Money Service Provider shall report same to FIU without delay but no later than 48 hours.

**9.12**. Any transaction reported under ***para 9.11*** shall, where appropriate, be discontinued until otherwise directed by FIU

**9.13**. Mobile Money Service Provider shall, irrespective of any exemptions under these directives, obtain evidence of identity at the commencement of every business relationship with a customer and in every significant, large and unusual financial transaction carried out, conducted or facilitated by a Mobile Money Service Provider.

**9.14**. Where a transaction is to be carried out by trust the Mobile Money Service Provider shall carry out the necessary level of identification and verification to ensure that the trustees are properly identified by obtaining details including but not limited to their names, occupation, residential addresses, postal addresses and any further particulars necessary for the profiling of the trustees and ensure that these are authenticated by obtaining publicly available document.

**9.15**. In addition to the information required under ***para 9.14***, Mobile Money Service Provider shall obtain copies of the most recent bank statement of trustees contemplated thereby and carry out the necessary level of verification and identification in order to ensure that the beneficiaries, settlors and persons that have control over the trust are in existence, and also to ensure that the beneficial owners are not in any way connected with money laundering, financing of terrorism, or any unlawful activity.

**9.16**.When a transaction is carried out by trustees through a Mobile Money Service Provider, the Mobile Money Service Provider, shall ensure that they carry out the necessary level of identification and verification to ensure that the beneficial owners exist by obtaining their details including but not limited to their names, postal addresses, residential addresses, email addresses, phone numbers and any further particulars necessary in the profiling of the beneficial owners contemplated by this paragraph.

9.17. When a transaction is carried out by trustees through a Mobile Money Service Provider, the Mobile Money Service Provider shall without prejudice to *para 9.16* obtain copies of the most recent bank statement of the beneficiary and any other document showing the financial status of the beneficiary.

9.18. Mobile Money Service Provider shall without prejudice to *paras 9.16 and 9.17* enquire about the intended use of the funds by the beneficiary contemplated thereby to ensure that the funds transmitted would not be diverted to fund terrorism or any unlawful activity and to ensure that the trust deed is not used as a conduit to transmit criminal proceeds.

9.19. Every Mobile Money Service Provider conducting, carrying out or facilitating a transaction involving a trust must obtain a copy of the deed that created the trust contemplated by *paras 9.14 – 9.18* of these directives.

## 10.00. RISK-BASED APPROACH IN RELATION TO POLITICALLY EXPOSED PERSONS.

10.01. If a Mobile Money Service Provider shall commence a business relationship with a Politically Exposed Person, the Mobile Money Service Provider shall carry out enhanced due diligence in relation to the identification requirement of the customer.

10.02. Without prejudice to *para 10.01* every Mobile Money Service Provider shall put in place appropriate risk management systems to determine whether a potential or existing customer or a beneficial owner or principal in a relationship or transaction is a Politically Exposed Person and shall subject same to enhanced due diligence as stipulated by the Act, any other law, regulation, directive or guidelines in force.

10.03. Every Mobile Money Service Provider in determining whether to commence a business relationship or to continue an existing relationship with or carry out, conduct or facilitate a transaction for or on behalf of a politically exposed person must seek sufficient information about the source of funds of the customer, the beneficial owners

thereof and any further particulars that may aid the Mobile Money Service Provider in complying with the enhanced due diligence requirement under the Act, with respect to the customer so that the Mobile Money Service Provider would be able to determine the level of risk posed by any relationship that may eventually come into being.

**10.04**. Where a Mobile Money Service Provider receives a request from a politically exposed person for the establishment of a business relationship or the carrying out, conduct or facilitation of a transaction, the decision to honour or reject the request must, subject to ***para 10.03*** be taken at the senior management level of the Mobile Money Service Provider.

**10.05**. If an existing customer of a Mobile Money Service Provider shall subsequently become or be identified as a politically exposed person, the decision to continue with the business relationship must subject to ***para 10.03*** be taken at the senior management level of the Mobile Money Service Provider.

**10.06**. In determining the suitability of a foreign politically exposed person for the commencement of a business relationship, the continuation of an existing relationship or the carrying out, conduct or facilitation of a transaction the Mobile Money Service Provider must identify the countries with which the politically exposed person has financial relationships and determine their level of vulnerability to corruption, money laundering, terrorism financing and any other factor or parameter incidental or ancillary thereto and shall apply enhanced due diligence measures thereof.

## 11.00. RISK-BASED APPROACH IN RELATION TO FUNDS TRANSFERS

**11.01**. Every Mobile Money Service Provider shall have measures in place to prevent terrorists and other criminals from having unfettered access to fund transfers for moving their funds to be sure that the fund transfer facilities they provide are not used for laundering proceeds of crime, financing terrorism, or any act or conduct incidental or ancillary thereto.

**11.02**. Every Mobile Money Service Provider that provides cross-border fund transfer shall ensure that the transfers are accompanied by accurate and meaningful originator information such as address, national identity number, customer identity number, date and place of birth and any further particulars that would aid the Mobile Money Service Provider in ascertaining the level of risk posed by the originator in relation to money laundering and terrorism financing.

**11.03**. Without prejudice to ***para 11.02*** every Mobile Money Service Provider involved in fund transfer shall ensure that the information accompanying the domestic fund transfers include originator information as if it were cross-border fund transfer.

**11.04**. Without prejudice to ***para 11.03*** if the originator information contemplated thereby shall make available to beneficiary Mobile Money Service Provider and competent authorities the Mobile Money Service Provider involved shall only include the account number or a unique identifier which will permit the transaction to be traced back to the originator.

**11.05**. If a Mobile Money Service Provider shall be involved in the processing of an intermediary element of either a domestic or cross-border fund transfer or domestic fund transfer, the Mobile Money Service Provider involved shall ensure that all originator information that accompanies a fund transfer is retained with the transfer.

**11.06**. Every beneficiary Mobile Money Service Provider shall have risk-based approach procedures in place to identify fund transfers lacking complete originator information in accordance with section 31 of the Anti-Money Laundering and Combating of Financing of Terrorism Act 2012.

## 12.00. DUTY TO IMPLEMENT ADEQUATE MEASURES TO PREVENT THE USE OF MOBILE MONEY SERVICES FOR ILLEGAL ACTIVITIES

**12.01**. Every Mobile Money Service Provider shall ensure that the designed and implementation of its mobile money model minimizes risk for abuse and provides the means to detect suspicious activities and report same to FIU.

**12.02**. In order to mitigate the risk of fraudulent and criminal activities, every mobile money service provider shall ensure a minimum that complete "end-to-end" electronic audit trails in place that provides a complete and total record of-

(a) funds received by agents;

(b) funds distributed by an agent;

(c) a complete record of all transfers undertaken by a participant;

(d) a complete record of all funds received by a participant;

(e) complete electronic records of all funds transfers and receipts undertaken within any service providers' products and services that will be available to FIU as required or on demand.

## 13.00. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

**13.01**. Every mobile money service provider shall upon recognising that a financial transaction and any other unlawful activities that bears the indicia of a suspicion of being connected with money laundering, terrorism financing or any unlawful act or conduct incidental or ancillary thereto, shall report within 48 hours after forming an objective opinion to FIU stating the parameters based on which the suspicion is raised, setting out the report in the format as required by FIU.

## 14.00. CURRENCY TRANSACTION REPORT (CTR)

**14.01** Where a mobile money service provider shall have conducted, carried out or facilitated a transaction for or on behalf of natural person and the transaction as maybe determined by FIU in Leones or its equivalent in foreign currency, the mobile money service provider, shall file a report of the transaction with FIU in the format as required by FIU.

**14.02** Without prejudice to ***para 14.01***, where a mobile money service provider shall have conducted, carried out or facilitated a transaction for or on behalf of a corporate body and the transaction as maybe determined by FIU in Leones or its equivalent in foreign currency the mobile money operator or service provider, shall file a report of the transaction with FIU in the format as required by FIU.

**14.03**. Without prejudice to ***para 14.01 and 14.02***, where the cumulative worth of Multiple currency transactions conducted for or on behalf of a natural person during a period ranging between 1 hour and 24 hours equal or exceed as maybe determined by FIU in Leones or its equivalent in foreign currency the Compliance Officer shall file a report on the transaction with FIU in the format as required by FIU.

**14.04**. Without prejudice to ***para 14.01, 14.02 and 14.03***, where the cumulative worth of Multiple currency transactions conducted for or on behalf of a corporate body during a period ranging between 1 hour and 24 hours equal or exceed as maybe determined by FIU in Leones or its equivalent in foreign currency the Compliance Officer shall file a report on the transaction with FIU in the format as required by FIU.

## 15.00. FOREIGN TRANSACTION REPORT (FTR)

**15.01**. Every Mobile Money Service Provider shall file with FIU a report of every foreign transaction involving the outflows and inflows of money or money's worth into and out of Sierra Leone in the template circulated to reporting entities in accordance to section 41 and 42 of the Anti-Money Laundering and Combating of Financing of Terrorism Act of 2012 and paragraph 23 of the Directives and Guidelines for Financial Institutions.

**15.02**. The obligation imposed on Mobile Money Service Providers under ***para 15.01*** shall not absolve any Mobile Money Service Provider from the obligation to report suspicious transactions to FIU whenever they are recognised.

**15.03.** Reports under ***para 15.02*** shall be forwarded by the Mobile Money Service Provider to FIU as shall be prescribed by FIU.

15.04. Where a Mobile Money Service Provider knows, ought to have known or has reasons to suspect that an investigation into a transaction is to be commenced by FIU, other competent authority or a regulatory body, the Mobile Money Service Provider shall preserve all data and records kept and maintained under these directives, of every customer connected directly or indirectly with the transaction under investigation until otherwise ordered by FIU.

15.05. Every Mobile Money Service Provider shall maintain a register of all enquiries and investigations on accounts operated or transactions conducted or facilitated thereby for or on behalf of a customer where the investigation is conducted by FIU or other competent authorities.

15.06. The register of enquiries contemplated by ***para 15.05*** shall contain details including but not limited to the date and nature of the enquiry, the details of the accounts or transactions involved, identification details of the persons or entities involved, the outcome of each investigation or enquiry and any other particulars that would facilitate the reconstruction and analysis of each case on the register.

15.07. Every Mobile Money Service Provider shall ensure that every register kept and maintained under ***paras 15.05 and 15.06*** is preserved for at least five years.

15.08. When an investigation into a transaction linked to a register kept and maintained under ***paras 15.05 and 15.06*** shall be commenced by FIU, other competent authority or regulatory body FIU, other competent authority or regulatory body may request the institution having control or possession of the register to preserve same until it is instructed otherwise by FIU, other competent authority or regulatory body.

15.09. Where a Mobile Money Service Provider knows, ought to have known or has reasons to suspect that an investigation into a transaction linked to a register kept and maintained under ***paras 15.05 and 15.06*** is to be commenced by FIU, other competent authority or a regulatory body the Mobile Money Service Provider shall preserve the register until otherwise instructed by FIU other competent authority or regulatory body.

## 16.00. ADMINISTRATIVE PENALTIES FOR VIOLATIONS OF THESE DIRECTIVES AND GUIDELINES

**16.01.** without prejudice to ***paragraph 17.01*** and any other laws, regulations, Directives and Guidelines in force where a mobile money service provider shall commit any act or omission in violation of these Directives the defaulting mobile money service provider shall pay to FIU administrative penalties that are dissuasive and proportionate.

Provided that any administrative penalties to be imposed on a defaulting mobile money service provider by FIU under these Directives shall be determined by FIU and communicated to the defaulting financial institution within a reasonable time.

**16.02.** Without prejudice to ***paragraph 16.01*** and any other law, regulations, Directives and Guidelines in force any administrative penalties imposed by FIU on a defaulting mobile money service provider shall be consistent with the Schedule of Penalties depicted by **Appendix A**

**16.03**. Without prejudice to ***paragraphs 16.01 and 16.02*** and any other laws, regulations, Directives and Guidelines in force any penalty FIU imposed pursuant to these Directives shall be equal to NLe10.00

**16.04**. Where a Mobile Money Service Provider shall fail to pay a fine imposed by the FIU in compliance with ***Paragraphs 16.01, 16.02 and 16.03*** within the time stipulated therefore this shall be a compliance violation and the defaulting Mobile Money Service Provider shall be liable to pay a fine equal to the amount imposed for every day the violation contemplated in this Paragraph continues without prejudice to any civil, administrative or criminal proceedings that may be instituted by the UNIT or other competent and supervisory authorities.

**16.05.** Without prejudice to **paragraphs 16.01, 16.02, 16.03, 16.04, 16.05 and 16.06**, where a mobile money service provider shall repeat any violation contrary to the provisions of these Directives and Guidelines, the Act or any other applicable law, Regulations in force for which the defaulting mobile money service provider had been previously penalised in compliance with these Directives or any other law in force, the Unit may impose a fine equal to or greater twice the penalty previously imposed for the

same or similar offence without prejudice to any other administrative, civil or criminal proceedings that may be instituted by the supervisory authorities or other competent authorities.

16.06. Without prejudice to ***paragraph 16.01, 16.02 and 16.03*** the imposition of administrative penalties by FIU on a defaulting mobile money service Provider shall not preclude the supervisory authority of the defaulting mobile money service provider from imposing separate penalties in compliance with the rules/directives applicable to the mobile money service provider as may from time to time be issued by the supervisory authorities or any applicable laws or regulations.

16.07. Without prejudice to these Directive or any other law, regulations, Directives and Guidelines in force, any penalty imposed on defaulting mobile money service provider shall not be a bar to FIU, competent authorities and supervisory authorities instituting criminal, civil and other proceedings against the defaulting mobile money service provider.

## 17.00. MISSCELLANEOUS PROVISIONS

17.01. These Directives and Guidelines shall be legally enforceable in accordance with the provisions of the Act.

17.02. FIU in consultation with the supervisory authorities may amend or replace any or all the paragraphs in these Directives and Guidelines in response to the operational dynamics of mobile money service providers or changes in the trends of money laundering, terrorism financing, proliferation financing or predicate offences.

17.03. Where there is a conflict between the provisions of the Act and other enactments in force and these Directives and Guidelines, the Act or other enactment in force shall prevail.

17.04. Without prejudice to the general obligations of mobile money service providers under these Directives, FIU in consultation with the supervisory authority may issue

other or further Directives, amend or repeal any paragraph of these Directives as the evolving operational circumstances in the financial space as they relate to mobile money service providers.

## APPENDIX A: SCHEDULE OF PENALTIES

| SECTION OF THE DIRECTIVES | OBLIGATION | COMPLIANCE VIOLATION | MINIMUM NUMBER OF PENALTY UNITS |
|---|---|---|---|
| 4.00 | Duty to keep records of transactions. | Failure to comply with this section. | 500 |
| 5.00 | Duty to carry out mobile money payment processes. | Failure to comply with this section. | 400 |
| 6.00 | Duty to carry out proper KYC/CDD requirements | Failure to comply with this section. | 300 |
| 7.00 | Duty to appoint a compliance officer | Failure to comply with this section. | 500 |
| 8.00 | Duty to ensure that adequate risk management is in place | Failure to comply with this section. | 400 |
| 9.00 | Duty to carry out a risk-based approach | Failure to comply with this section. | 400 |
| 10.00 | Duty to carry out a risk-based approach in relation to politically exposed persons | Failure to comply with this section. | 500 |
| 11.00 | Duty to carry out risk-based approach in relation to funds transfers | Failure to comply with this section. | 300 |

| | | | |
|---|---|---|---|
| 12.00 | Duty to implement adequate measures to prevent the use of Mobile Money Services for illegal activities | Failure to comply with this section. | 300 |
| 13.00 | Duty to recognize and report suspicious transactions | Failure to comply with this section. | 500 |
| 14.00 | Duty to report currency transaction | Failure to comply with this section. | 400 |
| 15.00 | Duty to report foreign transaction | Failure to comply with this section. | 400 |

6th December 2023

Mr. Sheku Ahmed Fantamadi Bangura
Minister of Finance
Chairman Inter-Ministerial Committee
For and on behalf of the Financial Intelligence Unit

Mr. David N. Borbor
Director
Financial Intelligence Unit, Sierra Leone
For and on behalf of the Financial Intelligence Unit

Made this 6th day of December 2023