

FINANCIAL INTELLIGENCE UNIT, SIERRA LEONE



DIRECTIVES & GUIDELINES FOR FINANCIAL INSTITUTIONS ON THE PREVENTION OF
MONEY LAUNDERING/TERRORISM FINANCING

NO: FIU/001/16

ISSUED BY
THE FINANCIAL INTELLIGENCE UNIT

TABLE OF CONTENT

INTRODUCTION.....	3
1.00.INTERPRETATION.....	3
2.00. SCOPE OF THE DIRECTIVES AND GUIDELINES.....	5
3.00. THE DUTY TO ENSURE CUSTOMER DUE DILIGENCE (CDD).....	5
4.00. DUE DILIGENCE IN RELATION TO EMPLOYEES OF FINANCIAL INSTITUTIONS.....	8
5.00. DUE DILIGENCE IN RELATION TO JURISTIC PERSONS.....	9
6.00. DUE DILIGENCE IN RELATION TO SUBSIDIARIES AND BRANCHES OF CORPORATIONS DOMICILED OUTSIDE SIERRA LEONE.....	10
7.00. THE DUTY TO TAKE A RISK-BASED APPROACH.....	11
8.00. THE RISK-BASED APPROACH IN RESPECT OF INTERMEDIARIES.....	15
9.00. RISK-BASED APPROACH IN RELATION TO NON-FACE-TO-FACE CUSTOMERS.....	16
10.00. RISK-BASED APPROACH IN RELATION TO POLITICALLY EXPOSED PERSONS.....	17
11.00. RISK-BASED APPROACH INRELATION TO WIRE TRANSFERS ANDFUNDS TRANSFERS.....	18
12.00. PROHIBITION OF SHELL BANKS.....	19
13.00. DUE DILIGENCE IN RELATION TO CORRESPONDENT BANKING.....	20
14.00. THE DUTY TO CO-OPERATE WITH COMPETENT AUTHORITIES.....	24
15.00. SUPERVISORY AUTHORITIES.....	24
16.00. THE ROLE OF BOARD MEMBERS AND SENIOR MANAGEMENT OF FINANCIAL INSTITUTIONS.....	25
17.00. STEPS INVOLVED IN THE VERIFICATION EXERCISE.....	25
18.00 OPENING ACCOUNT FOR PARTNERSHIPS AND OTHER UNINCORPORATED BUSINESSES.....	28
19.00. ACCOUNTS FOR EXECUTORS TRUSTEES ETC.....	29
20.00. THE REQUIREMENT FOR INTERNAL MANAGEMENT AND CONTROL MECHANISMS.....	30
21.00. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS.....	32
22.00. CURRENCY TRANSACTION REPORT (CTR).....	32
23.00.FOREIGN TRANSACTION REPORT (FTR).....	32
24.00. THE OBLIGATION TO KEEP RECORDS OF TRANSACTIONS.....	34
25.00.THE OBLIGATION TO FREEZE ASSETS OF DESIGNATED PERSONS AND ENTITIES.....	36
26.00. MISCELLANEOUS PROVISIONS.....	37
APPENDICES.....	38

INTRODUCTION

These Directives and Guidelines are issued by the Financial Intelligence Unit (Hereinafter referred to as "**The Unit**") pursuant to Section 133 (1) of the Anti-Money Laundering and Combating of Financing of Terrorism Act, 2012 Act No 2 of 2012 (Hereinafter referred to as "the Act") in consultation with the Bank of Sierra Leone (Supervisory Authority for financial institutions & Currency Exchange and Transmission businesses) and the Sierra Leone Insurance Commission, (Supervisory Authority for the insurance industry) as provided for under Section 13 (1) (j) of the Act in order to ensure compliance with the provisions thereof and to guarantee full cooperation with the competent authorities in the fight against money laundering and the financing of terrorism.

1.00. INTERPRETATION

"AML/CFT" means Anti-Money Laundering and Combating of Financing of Terrorism.

"Applicant for business" means party that applies to a financial institution praying for the establishment of a continuing business relationship or the conduct of a one-off transaction.

"CDD" shall mean Customer Due Diligence.

"CISU" shall mean Central Intelligence and Security Unit.

"Competent Authorities" shall include The Attorney-General, Director of Public Prosecutions, Director General of CISU, Inspector General of Police, Commissioner Anti-Corruption Commission, Governor Bank of Sierra Leone (BSL), Director of the Unit, any law enforcement agency and any person exercising such powers on behalf of these authorities.

"Compliance Officer" shall have the meaning ascribed in section 35, PART VII of the Act

"Designated persons and entities" shall have the meaning ascribed to it in Regulation 1 of the Terrorism Prevention (Freezing of International Terrorist Assets and Related Measures) Regulations 2013

"ECOWAS" shall mean Economic Community of West African States.

"Entry" shall mean the beginning of either a one-off transaction or a continuing business relationship that triggers the requirement of identification or verification under these directives.

"Established business relationship" shall mean a business relationship where an institution has obtained and maintained in accordance with these Directives satisfactory evidence of identity of the person who in relation to the formation of that business relationship was the applicant for business.

"High Risk Countries" refers to countries or jurisdictions which do not or insufficiently apply the FATF Recommendations, designated as High Risk and Non-Cooperative Jurisdictions and those known to have inadequate AML/CFT laws and regulations. It shall also refer to those countries or jurisdictions notorious for particular types of crimes, such as drug trafficking, human trafficking, child pornography, fraudulent activities, robbery etc.

"High Risk Regions" refers to regions within a country notorious for certain types of crimes connected with money laundering, terrorism activities, and other criminal behaviour.

"Key-staff" refers to any employee of a financial institution who deals directly with customers/clients and/or their transactions.

"Money Laundering" refers to the offences as defined by Section 15 of the Act.

"One-off transaction" shall mean any transaction carried out other than in the course of an established business relationship.

"Politically Exposed Persons" shall have the meaning ascribed to it by Section 1 of the Act.

"Reporting Entity" refers to individuals and institutions contemplated by Section 1 of the Act and PART I of the Second Schedule thereto (hereinafter referred to as "Financial Institution

"Significant transactions"-shall mean *in the case of financial institutions*, transaction involving pecuniary resources equal to or greater than Le30, 000,000.00 (or its equivalent in foreign currency). It does not matter whether it is a transaction or the aggregate of a series of linked transactions. In the case of casinos and gambling establishments, a transaction is significant where the exchange of chips or token involves an amount equal to or greater than Le5, 000,000.00 (or its equivalent in foreign currency).

"Supervisory Authorities" shall include the Unit, Bank of Sierra Leone, Sierra Leone Insurance Commission and all bodies or agencies established under an Act of parliament or any other law that regulates the conduct of individuals or organisations in an industry or a profession relevant to the implementation and enforcement of the Act.

"Terrorism financing" refers to the offence in Section 16 of the Act.

"Terrorist act" shall have the meaning ascribe to it in Section 1 of the Act.

"The Act" for the purpose of these Directives shall mean the Anti-Money Laundering and Combating of Financing of Terrorism Act, 2012, Act No 2 of 2012.

"The Director" shall mean the Director of the Unit.

"The Unit" for the purpose of these Directives shall mean the Financial Intelligence Unit, Sierra Leone.

"Unlawful activity" shall have the meaning ascribed to it in Section 1 of PART 1 of the AML/CFT Act 2012.

"UNSCR" shall mean United Nations Security Council Resolution.

2.00. SCOPE OF THE DIRECTIVES AND GUIDELINES

2.01. These Directives shall apply to financial institutions and relevant businesses listed in Part I of the First Schedule of the Act, and any other institution and activity specified by the Unit by order made by statutory instrument

2.02. Financial Institutions shall constantly remain vigilant in preventing criminals from making use of their organisations and any product or facilities offered by them for the purposes of money laundering or terrorism financing.

3.00. DUTY TO ENSURE CUSTOMER DUE DILIGENCE (CDD)

3.01. Financial Institutions shall establish and maintain internal procedures, policies and controls to prevent money laundering and terrorism financing, such as customer due diligence and shall ensure that their employees internalise these procedures in order to enable them deal appropriately with transactions that pose the risk of money laundering and financing of terrorism.

3.02. Financial Institutions shall not enter into a business relationship or carry out a significant occasional or one-off transaction unless it has fully implemented the Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures and purpose of all complex unusual large transactions and all unusual patterns of transactions hence shall examine as far as reasonably possible, the background and purpose of all complex, unusual large transactions and unusual patterns of transactions which have no apparent economic justification or lawful purpose.

3.03. Financial Institutions shall put in place internal mechanisms in order to ensure that key staff understand the basics of the AML/CFT regime and react effectively to suspicious circumstances by reporting them to the appropriate in-house compliance officer, with a view to reporting same to the Unit.

3.04. Every Financial Institution shall develop an Institutional Procedure Manual relating to entry, verification and records consistent with the AML/CFT regime in force and geared towards the detection and prevention of money laundering and the financing of terrorism.

3.05. Financial Institutions shall ensure that CDD procedures are implemented preparatory to the commencement of business relationship and when any significant transaction is conducted on behalf of customers or non-customers using the service of a Financial Institution for specific businesses or transactions. Financial Institutions shall conduct ongoing CDD until the business relationship is terminated or the specific financial transaction is concluded.

3.06. Every financial institution shall design and implement the appropriate verification and identification procedures to ensure that every existing or prospective customer can be easily located in the event that the financial institution or a competent authority shall require his or her contact for the purpose of business or an investigation.

3.07. Where two or more parties shall operate an account in a financial institution, the financial institution shall implement the appropriate verification and identification protocols in respect of each of the parties operating the account and where there is an agency relationship between the parties, the financial institution must sufficiently identify the agent and the principal.

3.08. Where a financial institution is satisfied that the signatory to an account is an agent acting on the instructions of a principal each transaction in the account carried out by the signatory must be closely scrutinised to ensure that it is specifically authorised by the principal and that it does not pose a threat of money laundering and terrorism financing.

3.09. If a financial institution shall in carrying out a verification and identification exercises under *paras 3.05 – 3.08* have reasons to suspect that a scenario may directly or indirectly involve money laundering and or terrorism financing the financial institution shall report the suspicious circumstance to the Unit without delay but not later than 48 hours.

3.10. Where a financial institution reports a transaction under *para 3.09* of these directives or any other law, regulation, directive or guideline in force, the Unit may direct that the financial transaction reported be suspended for any period not exceeding 10 working days. Provided that the Unit May before the effluxion thereof or so soon thereafter apply to the High Court for an extension of time beyond the 10 day period stipulated hereby giving justifications thereof.

3.11. Every financial institution shall apply customer due diligence measures to prospective and existing customers including:

(a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customer, their business and risk profile including where necessary, the source of funds and

(b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records (such as customer's place of employment, the marital status, citizenship, line of business, address) particularly for higher risk categories of customers.

3.12. Financial institutions shall not allow minors to open accounts in their own names.

Provided that nothing in these directive shall preclude a adult operating an account as a trustee for minor

Provided also that all verification and identification procedures under the Act, any other law, regulation, directive or guidelines in force having within its spirit and intendment the combating of money laundering and financing of terrorism shall be carried out to ensure that any person operating as a trustee under this paragraph is not in any way involved in money laundering, terrorism financing or any act or conduct incidental or ancillary thereto and to ensure that any trust account operated under any law, regulation, directive or guideline in force is not used for the purpose of money laundering or the financing of terrorism.

3.13. If a trust account shall be operated under *para 3.12* the financial institution hosting that account shall implement all the verification procedure under the Act, any other law,

regulations, directive or guideline in force to ensure that the minor in trust for whom the account is operated is in existence and also to clearly establish the relationship between the trustee and the minor to show that there is sufficient legal justification for the creation of the trust account.

3.14. If a financial institution carrying out a verification and identification under *paras 3.12 and 3.13* shall suspect that a scenario has been created which bears the indicia of a suspicious transaction connected in whatever way with money laundering, financing of terrorism, or any other act or conduct incidental or ancillary thereto, the financial institution shall report the circumstances to the Unit without delay but not later than 48 hours.

Provided that where a financial institution shall report a transaction under *this paragraph* of these directives or any other law, regulation, directive or guideline in force, the Unit may direct that the financial transaction reported be suspended for any period not exceeding 10 working days.

Provided also that the Unit May before the effluxion thereof or so soon thereafter apply to the High Court for an extension of time beyond the 10 day period stipulated hereby giving justifications thereof.

3.15. No financial institution shall open or maintain an anonymous account and no customer of a financial institution shall be allowed to open, operate or maintain an account in fictitious names or numbers, addresses etc.

3.16. Every financial institution having carried out the necessary verification and identification exercise required by the Act, any other law, regulation, directive or guideline in force in respect of an existing or prospective customer under the rubric of customer due diligence shall store every set of data obtained from the exercise so that the financial institution would be able to verify when required that the customer has gone through the various AML/CFT protocols before the commencement of the business relationship by the financial institution.

3.17. As part of the customer due diligence procedure, and preparatory to the establishment of business relationship, financial institutions shall collect and verify the customer's bio-data generally, details of the customer's business or employment, source and origin of the funds the customer will be using in the business relationship with the financial institution, details of the relationship between signatories and the underlying beneficial owners, the expected level and type of transactions that will take place in the relationship.

3.18. Without prejudice to *para 3.17*, a financial institution in entering a business relationship with a customer must make clear and in a documented way the purpose of the relationship, the intended nature of the relationship, the types and volumes of transactions

to be carried out in the relationship, the type, source and origin of funds that will go through the system in the name of the customer and any further particulars that may help facilitate compliance with the Act, any other law, regulation, directive or guideline in force having within it the spirit and intendment of the Act.

3.19. Where a customer of a financial institution carries out separate transactions aggregating to a sum of money equal to or exceeding Le 30,000,000 (thirty million Leones) in several operations the financial institution must implement the relevant CDD measures to determine whether:

- a) The transactions are in any way linked;
- b) The transactions are deliberately split;
- c) The transactions involve domestic or cross-border wire transfer;
- d) The transactions have dramatically changed the economic circumstances of the customer; and
- e) The transactions would, by their nature, raise suspicion of money laundering and terrorism financing.

3.20. If a financial institution in carrying out the CDD measures under *para 3.20* shall determine that the transactions carried out by the customer have sufficient indicia to raise suspicion of money laundering and financing of terrorism the financial institution shall report same to the Unit without delay but not later than 48 hours.

Provided that where a financial institution shall report a transaction under this paragraph of these directives or any other law, regulation, directive or guideline in force the Unit may direct that the financial transaction reported be suspended for any period not exceeding 10 working days.

Provided also that the Unit May before the effluxion thereof or so soon thereafter apply to the High Court for an extension of time beyond the 10 day period stipulated hereby giving justifications thereof.

4.00. DUE DILIGENCE IN RELATION TO EMPLOYEES OF FINANCIAL INSTITUTIONS

4.01. Every Financial Institution shall have "KNOW YOUR EMPLOYEE (KYE)" procedures under which every financial institution shall conduct due diligence checks on potential employees to ensure that only fit and proper persons are employed.

4.02. The due diligence procedures under *para 4.01* shall be sustained during the tenure of the employees in every Financial Institution in order to keep track of employees' life styles and financial commitments so that the institution is able to detect or foresee the possibility of employees posing a risk of money laundering and terrorism financing.

4.03. Employees shall be at liberty to move from one financial institution to another within the limits of the law.

Provided that employees moving to other financial institutions shall not withhold the knowledge and information acquired during their previous employment about individuals and organisation suspected of involvement in money laundering and terrorism financing so that the subsequent employers do not, due to lack of knowledge, allow such individuals or organisations to use their facilities and products to carry out or facilitate money laundering and terrorism financing.

5.00. DUE DILIGENCE IN RELATION TO JURISTIC PERSONS

5.01. Every financial institution in entering a business relationship with a corporate body shall:

- a) Apply the necessary AML/CFT mechanisms to sufficiently identify those natural persons who are behind the formation of the corporation to ensure that the idea of forming the corporation was conceived by fit and proper persons;
- b) Carry out proper identification and verification exercise to ensure that those acting for the corporation are those legally authorised to do so either under the M & A of the company, under any other law or some agency relationship expressed in writing in compliance with the laws of Sierra Leone;
- c) Verify the legal status of the corporation by satisfying itself that all the legal processes and procedures necessary for incorporation and certification were followed and that all licencing and documentation requirements have been met;
- d) Carry out the verification and identification necessary to be satisfied that members of the corporation's governing body are fit and proper persons;
- e) Inquire into the financial standing of the corporation by obtaining copies of the corporation's most recent statements of account and audited financial statements; and
- f) Carry out due diligence procedures on the shareholders, particularly where the shareholders are acting as trustees or agents, identify the beneficial owners, verify the identity of such persons and ensure that there is a clear understanding of the structure of ownership in relation to the percentage of ownership or controlling shares held by each shareholder.

5.02. If the shareholders or managers, directors, and any other persons in control of the corporate body are non-Sierra Leonean nationals the financial institution shall take such measures as are necessary to ensure that they are not connected with money laundering, terrorism financing and offences predicate thereto by requiring them to obtain attestations from their embassies and /or a police clearance from the criminal investigations Department in their home countries.

5.03. The financial institution shall also take the necessary measures to ascertain the historical business track record of those foreign nationals and how they operated in their home countries and elsewhere prior to seeking a business relationship with the financial institution.

5.04. If an individual customer has a controlling interest in a company or any corporate body the financial institution must carry out due diligence on both the individual customer and the company to ensure that the company is not being used as a front to launder the proceeds of crimes nor as a conduit pipe for the terrorism financing.

5.05. Without prejudice to *para 5.01 (d)* a financial institution conducting, carrying out, dealing with or facilitating a transaction with a corporate body or a company shall verify and identify the beneficial owners thereof, who ultimately have controlling interest in the company unless the company is listed on the stock exchange or is a subsidiary of such a company.

6.00. DUE DILIGENCE IN RELATION TO SUBSIDIARIES AND BRANCHES OF CORPORATIONS DOMICILED OUTSIDE SIERRA LEONE.

6.01. Every Financial institution entering a business relationship with a branch or subsidiary of a corporate body domiciled outside Sierra Leone shall gather sufficient information about the corporate body so as to understand the nature and extent of business carried out by the corporation and hence the financial institution shall:

- a) Properly identify the promoters obtaining and recording details including but not limited to their names, residential addresses, official addresses, and postal addresses, details of their identity cards, passport, and any further particulars needed to ensure that those promoters were not involved in any suspicious or illegal activities; and
- b) Ensure that the company domiciled overseas and desirous of having a branch or subsidiary in Sierra Leone obtain an attestation from their embassies in Sierra Leone to be forwarded to the financial institution to ensure that the corporation is a legitimate business concern properly incorporated and certified in their country of domicile or origin.

6.02. Every financial institution shall upon receipt of an application for the creation of an account or establishment of a business relationship for or on behalf of a company registered outside Sierra Leone obtain and examine the resolution of the Board of Directors authorising the creation of the account or establishment of a business relationship with specific focus on those on whom authority is conferred to operate the account so that they can be properly identified and verified in accordance with the verification requirements for non-resident individual customers as outlined in these directives.

6.03. A financial institution shall in processing the application for the creation of an account or establishment of a business relationship under *para 6.02*:

- a) Carry out enhanced due diligence to verify the identities of those individuals who ultimately control the company;
- b) Obtain and examine evidence that the individuals representing the company have the necessary authority to do so and shall obtain and examine documents substantiating such authority; and,

c) Take every step necessary to ensure that all potential signatories to the account are accredited by the company.

6.04. Every financial institution shall in processing an application for the creation of a large corporate account obtain and examine certain documents as part of the verification exercise including but not limited to the following:

- a) Annual reports/audited financial statements;
- b) Description and place of principal line(s) of business, list of major business units, suppliers and customers, etc. where appropriate.
- c) Annual Minutes of the last Annual General Meeting
- d) Any other information or particulars necessary in the assessment of the viability and credibility of the company or corporate body

6.05. Every financial institution shall in carrying out the identification and verification under *paras 6.02, 6.03 and 6.04* of these directives or any other law or regulation in force shall forward a request to other institutions for the verification of information received during the identification exercise in the manner set out in **APPENDIX 3**.

7.00. THE DUTY TO TAKE A RISK-BASED APPROACH

7.01. Financial institutions shall in their internal control policy formulation and implementation in compliance with the AML/CFT 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 AML/CFT measures adopted will be proportionate to the level of risk posed by a particular customer, product, service, client, transaction or geographical factor involved.

7.02 Financial institutions shall conduct periodic reviews every six months) 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 in order that a determination be made by senior management as to whether the relationship should be continued.

Provided that all decisions regarding high risk relationships and the basis for these decisions shall be documented.

7.03. Financial institutions shall pay special attention to the Know Your Customer (KYC) regime when entering business relationship with a customer, hence financial institution must determine the level of risk posed by the customer before a decision is taken on whether to commence a relationship so that any AML/CFT measures adopted would be effective enough to counter any possible threat that may be posed by the potential customer.

7.04. Every financial institution 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.

7.05. Where a transaction involves the transmission of money from one jurisdiction to another the financial institution involved shall document the number of underlying transactions of each bulk transfer made to or through them by their customers so that the financial institution be certain that the number and average value of transactions is consistent with the level of business disclosed by the customer to the financial institution preparatory to the commencement of the business relationship and ensure that the behaviour of the client is carefully scrutinised in order to enable the financial institution to report any suspicion that the transaction may be connected in whatever way with money laundering or terrorism financing to the Unit without delay but not later than 48 hours.

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

7.07. Where a currency exchange or transmission business customer operates within high risk jurisdictions such as a financial corridor the financial institution 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 financial institutions 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.

7.08. Financial institutions 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.

7.09. Where the transaction involve a charitable organisation or the funds thereof are intended for charitable purposes the financial institution shall carry out enhanced due diligence to ensure that the charitable venture is not used as a front to launder proceeds of

crime or the otherwise legitimate income is not used to fund terrorism or any unlawful activity behind the veil of charity.

7.10. A financial institution carrying out or facilitating a transaction/business relationship involving charity or the 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 7.09** 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 financial institution for the purpose of verification and authentication.

7.11. If the verification and identification exercise carried out under **paras 7.09 and 7.10** reveals suspicious circumstances in relation to money laundering, financing of terrorism, or any unlawful activity the financial institution shall report same to the Unit without delay but no later than 48 hours.

7.12. Any transaction reported under **para 7.11** shall be discontinued until otherwise directed by the Unit.

7.13 Without prejudice to **para 7.14** enhanced due diligence shall not be mandatory in circumstances where information on the identity of the customer and the beneficial owner is publicly available or where adequate, checks and controls exist elsewhere in national systems.

7.14 Financial institutions shall ensure that when dealing with customers resident in other countries the exemption under **para 7.13** shall apply only to countries that have in place AML/CFT measures in compliance with the FATF Recommendations.

7.15. Financial institutions 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 financial institution.

7.16. Where a transaction is to be carried out by trust the financial institution 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.

7.17. In addition to the information required under *para 7.16*, financial institutions shall obtain copies of the most recent bankstatement 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.

7.18. When a transaction is carried out by trustees through a financial institution, the financial institution, 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.

7.19. When a transaction is carried out by trustees through a financial institution, the financial institution shall without prejudice to *para 7.18* obtain copies of the most recent bank statement of the beneficiary and any other document showing the financial status of the beneficiary.

7.20. Financial institutions shall without prejudice to *paras 7.18 and 7.19* 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 also to ensure that the trust deed is not used as a conduit to transmit criminal proceeds.

7.21. Every financial institution conducting, carrying out or facilitating a transaction involving a trust must obtain a copy of the deed that created the trust contemplated by *paras 7.16 - 7.20* of these directives.

8.00. THE RISK-BASED APPROACH IN RESPECT OF INTERMEDIARIES

8.01. Where a transaction is carried out through a financial institution by an intermediary on behalf of an underlying customer, both the intermediary and the underlying customer must be identified and verified.

8.02. Without prejudice to *para 8.01*, where the intermediary is a locally regulated institution and the account operated on behalf of the underlying customer is in the name of the institution verification of the institution shall not be mandatory.

Provided that the underlying customer contemplated by *para 8.01* must be verified by the financial institution for all purposes.

8.03. Without prejudice to *para 8.02* where the documentation is in the name of the underlying customer contemplated by *para 8.01* but the intermediary has power to operate any bank, securities or investment account, the intermediary must be verified.

8.04. If a financial institution shall suspect that there may be an undisclosed principal (either an individual or a corporation) to an alleged intermediary operating an account or carrying out a transaction therein with the prima facie indicia of an agent or trustee, the financial institution shall apply enhanced due diligence measures and monitor the activities of the customer to determine whether the customer is in fact merely an intermediary.

8.05. If through due diligence conducted under *para 8.04*, a principal is found to exist, the financial institution shall make further enquiries and shall forthwith subject the transaction to the enhanced due diligence verification and identification mechanisms.

8.06 Where the applicant for business is an advocate, notary public, certified public accountant and auditor or nominee registered as a professional and practising in Sierra Leone who is not acting on his own behalf the financial institution shall obtain from the applicant for business and examine a signed declaration to the effect that the applicant for business has the authority to act on behalf of the principal and be sure that the applicant is acting in his professional capacity.

8.07. Every financial institution shall in processing an application under *para 8.06* ascertain that the applicant for business has maintained a professional relationship with the principal for the immediate preceding three months.

Provided that If such relationship is not held the applicant for business shall present references satisfactory to the financial institution from at least two professionals who held such relationship with the principal.

8.08. Every financial institution processing an application under *para 8.06* must require that the applicant for business has obtained satisfactory evidence of identity of the principal.

8.09. The applicant for business shall at the determination of the professional relationship between himself and the principal inform the financial institution in writing stating the reasons for the determination of the relationship and any other information or particulars raising suspicion that the principal may be linked to or connected with money laundering, terrorism financing, or any unlawful conduct or activity.

8.10. Without prejudice to **para 8.09** and the obligations of reporting entities under the Act the applicant shall report any suspicious circumstance suggestive of the principal being involved in money laundering, terrorism financing or any unlawful act or conduct.

8.11 Where an applicant for business is a corporate body whose share capital is partly or totally held by nominees the financial institution processing the application shall not undertake or carry out any business with the applicant for business unless they obtain disclosure of the full details of the ultimate beneficiary or beneficiaries to the satisfaction of the financial institution

9.00. RISK-BASED APPROACH IN RELATION TO NON-FACE-TO-FACE CUSTOMERS

9.01. Where a financial institution is requested to open an account or carry out, conduct, or facilitate a financial transaction on behalf of a customer who shall not be available for personal interview for reasons including but not limited to the customer being resident outside Sierra Leone, the financial institution shall carry out enhanced due diligence and pay special attention to the risk of the customer using modern technological advancements to use the facilities provided by the financial institution for the laundering of criminal proceeds, financing of terrorism or any unlawful purpose carry out unlawful activities. This may be done by reference to recognised financial institutions 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 and ensure that the customer is not connected to money laundering, terrorism financing or any act or conduct incidental or ancillary thereto.

9.02. Every financial institution shall have in place procedures and processes to address any risk associated with non face-to-face business relationships or transactions, document such procedures and processes and forward same to the Unit for consideration and possible review.

9.03. If a financial institution shall carry out, conduct or facilitate a financial transaction on account of a non face-to-face customer the financial institution shall adopt ongoing due diligence throughout the duration of the relationship or the transaction.

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

10.01. If a Financial institution shall commence a business relationship with a Politically Exposed Person, the financial institution shall carry out enhanced due diligence in relation to the identification requirement of the customer.

10.02. Without prejudice to **para 10.01** every financial institution 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 financial institution 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 financial institution in complying with the enhanced due diligence requirement under the Act, with respect to the customer so that the financial institution would be able to determine the level of risk posed by any relationship that may eventually come into being.

10.04. Where a financial institution 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 honor or reject the request must, subject to **para 10.03** be taken at the senior management level of the financial institution.

10.05. If an existing customer of a financial institution 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 financial institution.

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 financial institution involved 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 WIRE TRANSFERS AND FUNDS TRANSFERS

11.01. Every Financial institution shall have measures in place to prevent terrorists and other criminals from having unfettered access to wire transfers for moving their funds so as to be sure that the wire 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 financial institution that provides cross-border wire 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 financial institution 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**, Cross-border wire transfers that are contained within batches shall, with the exception of money remitters be treated as domestic wire transfer.

11.04. Every financial institution ordering wire transfers shall retain all originator information contemplated by **para 11.02** and shall on request make such information available to competent authorities and to the beneficial financial institutions.

11.05. Without prejudice to **para11.03**, every financial institution shall ensure that non-routine transactions involving wire transfer are not batched where this would increase the risk of money laundering and terrorist financing.

11.06. Without prejudice to **para 11.02** every financial institution involved in wire transfer shall ensure that the information accompanying the domestic wire transfers include originator information as if it were cross-border wire transfer.

11.07. Without prejudice to **para 11.06** if the originator information contemplated thereby could be made available to beneficiary financial institutions and competent authorities by other means the financial institution involved shall only include the account number or a unique identifier which will permit the transaction to be traced back to the originator.

11.08. If an ordering financial institution shall receive a request either from a competent authority or a beneficiary financial institution for originator information required under **paras 11.02-11.07** the requested financial institution shall within 3 business days of receipt of the information make available the requested information to the competent authority or the beneficiary financial institution.

11.09. Every ordering financial institution in possession of originator information secured under **paras 11.02-11.07** shall retain the information for at least five years after end of business relationship or the specific transaction.

11.10. If a financial institution shall be involved in the processing of an intermediary element of either a domestic or cross-border wire transfer or domestic wire transfer, the financial institution involved shall ensure that all originator information that accompanies a wire transfer is retained with the transfer.

11.11. Where technical limitations prevent the full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution.

11.12. Every beneficiary financial institution shall have effective risk-based procedures in place to identify wire transfers lacking complete originator information.

11.13. Without prejudice to *paras 11.01- 11.07* and the general requirement for customer due diligence under the Act or any other law, the required verification and identification shall not be mandatory with regards to:

(a) Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction including withdrawals from a bank account through an automatic teller machine (ATM), cash advances from a credit card, or payments for goods and services.

(b) Transactions involving wire transfers where both the originator and the beneficiary are financial institution acting on their own behalf.

12.00. PROHIBITION OF SHELL BANKS

12.01. No individual or institution shall be allowed to establish aid, abet, or counsel the establishment of a shell bank in any part of Sierra Leone.

12.02. No individual or institution shall be allowed to run, operate or engage in any form of business whatsoever with a shell bank.

12.03. No financial institution shall be allowed to enter into, or continue a correspondent banking relationship with a shell bank.

12.04. No Financial institution shall be allowed to establish business relationship with respondent foreign financial institutions that allow their accounts to be used by shell banks.

13.00. DUE DILIGENCE IN RELATION TO CORRESPONDENT BANKING

13.01. If a financial institution shall be desirous of entering a correspondent banking relationship with a respondent Bank the financial institution shall apply the enhanced customer due diligence measures listed in section 35(1)(a)-(e) of the Act and gather sufficient information about the respondent bank to understand fully the nature of business of the respondent bank. This may be done by reference to recognised financial institutions or other governmental and no-governmental agencies having records of financial institutions to verify any information that would have been supplied by the respondent Bank for the purpose of the transaction and ensure that the respondent Bank is not connected with money laundering, terrorism financing or any act or conduct incidental or ancillary thereto.

13.02. No financial institution shall enter into or continue a correspondent banking relationship with a financial institution incorporated or domiciled in a jurisdiction in which it has no physical presence.

13.03. Without prejudice to *para 13.02*, no financial institution shall enter into or continue a correspondent banking relationship with a financial institution incorporated or domiciled in a jurisdiction which has no AML/CFT regulatory framework and is not affiliated with a financial regulatory body or in a country classified as a high risk jurisdiction by Sierra Leone or the Financial Action Task Force, GIABA or any member State thereof.

13.04. If a financial institution shall be desirous of entering or continuing in a correspondent banking relationship involving the keeping of "payable through accounts" the financial institution must carry out the necessary verification and identification to ensure that:

- a) The respondent financial institution has performed all the normal CDD obligations set out in these Directives and Guidelines on those of its customers that have direct access to the accounts of the corresponding financial institutions; and
- b) The respondent financial institution is able to provide relevant customer identification data upon request to the corresponding financial institution.

13.05 If a financial institution is desirous of entering into a correspondent banking relationship the financial institution shall obtain approval from senior management before establishing such a relationship.

13.06. Without prejudice to *para 13.05* no financial institution shall enter or establish a correspondent banking relationship without the approval of senior management expressed in writing.

13.07. In establishing a correspondent banking relationship, a financial institution shall in so doing document the respective responsibilities of both parties in the relationship.

13.08. Without prejudice to paras *13.05, 13.06 and 13.07*, the identification procedures required in the enhanced due diligence in relation to correspondent banking under Section 35(1)(a) of the Act shall not apply, unless where the transaction involved is by its nature suspicious in relation to:

- a) Cases not Requiring Third Party Evidence in Support;
- b) Exempt Institutional Applicants; and
- c) Cases where the applicant for business is one of the institutions regulated by the Bank of Sierra Leone (BSL) under the Banking Act, 2011 or the Other Financial Services Act, 2001 the Other Financial Services (Amendment) Act, 2013 or institutions regulated by the Insurance Commission under the Insurance Act, 2000 or their equivalents in other jurisdictions.

13.09. Without prejudice to *paras 13.05, 13.06 and 13.07* the verification to be carried out under Section 35(1) (a) of the Act in the exercise of enhanced due diligence shall not be mandatory in relationships involving small one-off transactions (whether single or linked) **Provided**, that any exemption under this paragraph shall not apply to cases where in the cause of the relationship it appears that two or more transactions, which appeared to have been small one-off transaction, are in fact linked and constitute a significant one-off transaction.

13.10. The exception under *para 13.09* shall apply to any transaction where an applicant for business shall pay or intend to pay money to a financial institution by post or electronic means or by means of telephone instructions, in respect of a non-paying account.

Provided that the exception under this Paragraph shall apply only if;

- a) It is reasonable in all the circumstances for payment to be made by the means contemplated by this paragraph and the payment is made through an account held in the name (s) of the paying account holder.
- b) The name of the applicant for business corresponds with the name(s) of the paying account holder(s)
- c) The receiving institution keeps records of the applicant's account details with other institutions and;
- d) The applicant for business is reliably introduced by an eligible regulated institution preferably in writing in the form depicted in **Appendix 2**.

13.11. Without prejudice to *para 13.10* the introduction under sub-paragraph (d) thereof shall be deemed reliable only if:

- i) The introducer is one of the eligible financial institutions or professional intermediaries from a recognised regulated institution subject to equal regulatory standards as those in Sierra Leone.
- ii) The receiving institution is satisfied that AML/CFT regulations in the correspondent's institution (where the correspondent institution is regulated in a foreign jurisdiction) include requirements equivalent in standards to those in the AML/CFT regulations of Sierra Leone.
- iii) The introducing institution is in good standing as a going concern and the introduction includes an assurance that that evidence of identity had been taken and recorded in accordance with the procedures of that institution and in compliance with FATF Recommendations.
- iv) The introducing institution has within its regime customer identification and verification procedures that meet the standard of those in the receiving institution.
- v) The introducing institution is not incorporated or domiciled in a country classified as non-co-operative by the FATF
- vi) There is no suspicion of money laundering, terrorism financing or any act or conduct incidental or ancillary thereto.

vii) Where the introducer of an applicant for business is either an overseas branch or member of the same group as the receiving institution and there is written confirmation or evidence of the relationship by the parent company or institution.

13.12. Where an applicant for business shall pay or intend to pay money to a financial institution by mail shots, off-the-page and coupon business placed over the telephone or by other electronic means the receiving institution shall keep records of how the transaction originated.

13.13. In determining whether an applicant for business shall be exempt under *paras 13.10 and 13.11* the receiving institution shall be entitled to receive on demand records from the introducing institution confirming that the verification of the customer introduced is carried out in a thorough and comprehensive way and in accordance with international standards relevant to the fight against money laundering and terrorism financing.

13.14. If a receiving institution shall upon receipt of the record under *para 13.13* be dissatisfied with the work done by the introducing institution the receiving entity shall carry out its own verification and identification to a level commensurate with the risk posed by the customer introduced.

13.15. Where a financial Institution shall in the course of a business relationship with a customer exempt from verification and identification under *paras 13.09, 13.10 and 13.11* have reasons to suspect that the relationship would be used for money laundering and terrorism financing the exemption with respect to the customer or the transaction shall cease to apply and the institution shall resort to enhanced due diligence and promptly report same to the Unit.

13.16. Every financial institution shall carry out verification and identification on their customers as part of its ongoing due diligence in response to changes in the customers' way of life, economic status, political status and other aspects of social status to determine whether any such changes is incidental or ancillary to money laundering andoffinancing terrorism.

14.00. THE DUTY TO CO-OPERATE WITH COMPETENT AUTHORITIES

14.01. Every financial institution shall comply promptly with requests directed to it by the Unit, other competent authorities or supervisory authorities in accordance with provisions of the Act, any other enactment, Regulations, Guidelines or Directives in force.

14.02. Every financial institution shall have in its manual process setting out the procedures and mechanisms for responding to requests directed to it by the Unit, other competent authorities or supervisory authorities for information relevant to the gathering

of intelligence on or investigation of suspicious financial transactions in relation to money laundering or terrorism financing, including but not limited to:

- (a) The procedures for the immediate searching of institutional records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with individual or organisation named in the request;
- (b) The processes involved in reporting promptly to the requesting authority on the outcome of the search; and
- (c) The mechanisms put in place to maintain the security and confidentiality of any such request.

14.03. Any procedural framework developed by a financial institution under *para 14.02* shall be submitted to the Unit and supervisory body for consideration and possible contribution.

15.00. SUPERVISORY AUTHORITIES

15.01. THE UNIT shall have supervisory or enforcement powers in respect of AML/CFT issues for any institution, industry, profession or organisation contemplated by the Act or any other law, regulation, directive or guideline in force dealing with issues related to money laundering and financing of terrorism, where

- a) The institution, industry, profession or organisation concerned does not have a designated supervisory authority.
- b) The designated supervisory authority fails to act in response to failure by an institution, industry, profession or organisation contemplated by the Act or any other law, regulation, directive or guideline to comply with their obligation under the Act.

15.02 THE BANK OF SIERRA LEONE shall be the designated supervisory authority for financial institutions, currency exchange and transmission businesses.

15.03. THE SIERRA LEONE INSURANCE COMMISSION shall be the supervisory authority for the insurance industry.

16.00. THE ROLE OF BOARD MEMBERS AND SENIOR MANAGEMENT OF FINANCIAL INSTITUTIONS

16.01. The Board of Directors and senior management of every financial institution shall have joint and several oversight responsibilities for the effectiveness of their financial institutions' AML/CFT framework to ensure that there is compliance with all the relevant laws, regulations, guidelines, directives and international standards and best practises by their financial institutions.

16.02. Directors and Senior Management shall at all times remain aware that the use of a group-wide policy shall not absolve directors and senior management of their individual and

corporate responsibility in ensuring that their institution's AML/CFT policy is appropriate and in compliance with AML/CFT laws, regulations, guidelines and directives in force.

16.03. Directors and members of senior management of every financial institution shall be held jointly and severally responsible for any failure of their financial institutions to comply fully with the AML/CFT laws, regulations, directives and guidelines in force.

16.04. The directors and members of senior management of every financial institution having subsidiaries in or outside Sierra Leone shall ensure that subsidiaries and branches of their financial institution including those located outside Sierra Leone comply with the AML/CTF Laws, regulations, directives and guidelines in force.

16.05. Directors shall be aware that where some or all of a financial institution's operational functions are outsourced, the financial institution retains full responsibility for compliance with the AML/CFT laws, regulations, directives and guidelines in force.

17.00. STEPS INVOLVED IN THE VERIFICATION EXERCISE

17.01. Verification shall be a cumulative process including but not limited to documents from independent sources such as birth certificates, national identity cards, passports, driver's licences, etc.

17.02. Financial institutions shall where the potential customer is a corporate body obtain identification details of the promoters of the company as if they were potential customers themselves including details of their nationalities and their sources of finance or income

17.03. Financial institutions shall when dealing with corporate entities contemplated by *para 17.02* obtain details of the formation and registration of the entity so as to ensure that:

- a) The promoters of the corporate body are fit and proper persons in the sense that they have no link to money laundering, financing of terrorism or any unlawful activity or conduct.
- b) The corporate entity is properly registered and incorporated under the laws of Sierra Leone or the laws of the country of domicile or origin (where the entity is incorporated outside Sierra Leone).
- c) The corporate entity is financially viable at the time it makes an application to establish a business relationship.

17.04. A financial institution shall when dealing with corporate entities run or controlled by non-Sierra Leonean Nationals take extra measures as dictated by the circumstances to ensure enhanced due diligence.

17.05. Where an application is made by an unincorporated association the financial institution to which the application is directed shall apply enhanced due diligence in the

process of identifying and verifying leading members of the organisation such as the executive and ex-officio members to ensure that they are fit and proper persons within the meaning of **Para 16.03** to ensure that

- a) They are not linked to or connected with money laundering, terrorism financing or any unlawful act or conduct.
- b) The organisation is financially viable at the times the application for business is made.

17.06. For the purposes of verification under this head, financial institutions shall obtain references from banks and other professional firms and such references shall be received directly from the banks and other professional firms and institutions capable of providing such references.

17.07. A Financial institution shall upon receipt of an application by an individual natural person for a business relationship carry out the verification and identification exercise seeking identification particulars including but not limited to those set out in **APPENDIX 1**

17.08. A financial institution in processing an application under **para 17.07** shall ensure that the applicant is referenced by a bank or any professional body, organisation recognised and registered under the laws of Sierra Leone and any other body or institution capable of providing such reference.

17.09. A financial institution in processing an application under **para 17.07** shall where the applicant is a foreign national carry out enhanced due diligence to ensure that:

- a) The applicant is not from a country which is not a member of the United Nations.
- b) The applicant is not in any way connected with money laundering, terrorism, terrorism financing or any other act or conduct incidental or ancillary thereto.

17.10. In addition to the verification under **para 17.09** a financial institution shall in processing an application thereunder require that the applicant sign a certification on the reliability and accuracy of the information supplied to the institution and attestation thereto signed by the ambassador of his country of origin or any other officer duly authorised to do so.

17.11. A financial institution shall upon receipt of a certification and attestation from a foreign embassy under **para 17.10**, verify to ensure that certification and attestations are authentic in all respect before including same in the CDD records of the foreign customer.

17.12. The financial institution shall on the failure of the customer to submit a certification or an attestation from his embassy under **para 17.10** after a reasonable time to be determined by the financial institution, or upon receipt of an attestation or certification under **para 17.10** which is suspected to have been forged, the financial institution shall prevent the applicant from conducting any business or transaction in their institution

without prejudice to their obligations to immediately file a suspicious transaction report to the Unit.

17.13. Where a financial institution receives an application for business from an applicant resident outside Sierra Leone the financial institution shall carry out the necessary verification and identification required by enhanced due diligence.

Provided that the verification details under this paragraph shall where the circumstances so permit be accepted when supplied by a reputable financial institution or professional body or institution recognised and registered under the laws of the applicant's country of residence.

17.14. Without prejudice to **para 17.13** a financial institution in processing an application filed by an applicant resident outside Sierra Leone shall require that the applicant submit a police clearance issued by the Criminal Investigation Bureau of the country of residence to ensure that the applicant has no criminal records in his country of residence.

17.15. The financial institution shall require that all documents to be submitted by an applicant outside Sierra Leone under **para 17.13** and **17.14** must be certified by the embassy of the country of residence with an attestation thereto signed and sealed by the ambassador or any other person duly authorised to do so.

17.16. The financial institution shall, upon failure of an applicant resident outside Sierra Leone to submit the necessary documents certified and attested to under **paras 17.13, 17.14 and 17.15**, or upon receipt of any document in respect of the applicant which is suspected to have been forged, prevent the applicant from conducting any business with the financial institution without prejudice to the obligation to immediately submit a suspicious transaction report to the Unit.

17.17. A financial institution in processing an application for the creation of joint account shall ensure that the procedures set out for resident and non-resident account apply to all applicants in whose names the account is to be generated.

18.00 OPENING ACCOUNT FOR PARTNERSHIPS AND OTHER UNINCORPORATED BUSINESSES

18.01. A financial institution shall upon receipt of application for the creation of accounts for unincorporated association obtain the identification details of all members in line with the requirements for personal customers as outlined in **APPENDIX 1**.

18.02. The financial institution shall in processing an application under **para 18.01** ensure that the aims and objectives of the association are clearly outlined and understood so as to

be confident that the organisation or members thereof are not in any way connected with money laundering, terrorism financing or any unlawful act or conduct.

18.03. Where the organisation applying for business under **para 18.01** is a partnership the financial institution in processing the application shall ensure that they obtain and carefully examine:

- a) The partnership deed;
- b) Documents relating to the identification and verification of individual partners as outlined in **APPENDIX 1**;
- c) A copy of the mandate from the partnership or unincorporated business authorizing the establishment of the business relationship and confirmation of any authorized signatories;
- d) Documents connected to the formation and registration of the business; and
- e) Any other documents that may be necessary for the proper effective and reliable identification and verification of the association and members thereof.

18.04. A Financial institution shall in processing an application for the establishment of business relationships with clubs, societies and charities, apply enhanced due diligence to ascertain the purpose of the organization.

18.05 A financial institution processing an application for the establishment of a business relationship with organisations mentioned in **para 18.04** shall obtain and examine

- a) The constitution of the organisation
- b) The certificate of registration of the organisation issued by the Registrar-General (where the organisation is indigenous) or its equivalent issued in a foreign jurisdiction (where the organisation is of a foreign origin)
- c) Information relating to the organisation's source of funds
- d) Any further information necessary for the proper, effective and reliable identification of the organisation and members thereof.

18.06. Without prejudice to **para 18.05** every financial institution shall when dealing with Charitable and other non-profit oriented organisations conduct a special study of the promoters of the organisation.

19.00. ACCOUNTS FOR EXECUTORS TRUSTEES ETC

19.01 In establishing a business relationship for the purpose of administering the estate of a deceased person the identities of the executors and administrators shall be verified in accordance with these Directives and Guidelines.

19.02 Without prejudice to **para 19.01** the verification of identity shall not be mandatory where payment from an established bank account in the deceased's name is being made to

the executor or administrator in accordance with the Grant of Probate or Letters of Administration.

19.03. Without prejudice to *para 19.02*, nothing in these Directives and Guidelines shall absolve a financial institution from their obligation to carry out identity verification of beneficiaries receiving payments on the instructions of an executor or administrator in accordance with the identification and verification requirements as set out in these Directives.

19.04. Without prejudice to *para 19.02*, if any suspicion is raised about the nature or origin of assets comprising an estate being devolved or administered the process of administration or devolution shall be discontinued without precluding the obligation to file a suspicious transaction report to the Unit

19.05. Where a financial institution is to conduct a transaction of trust involving settlement and guarantee, the financial institution shall verify the identity of every settlor, guarantor or any person adding assets to the trust in accordance with the procedures relating to the verification of identity of clients and shall thereupon obtain and examine data including but not limited to the following:

a) the name, address, business, trade or occupation of the settlor or any person transferring assets to the trust and other information or particulars relevant to the adequate and reliable identification of same in accordance with the procedures relating to the verification of client identity outlined in these Directives;

b) The name, address, business, trade and occupation of every beneficiary, and any other information or particulars relevant to the adequate and reliable identification and verification of same in accordance with the procedures relating to the verification of client identity outlined in these directives.

c) The name, address, business, trade and occupation of the protector and evidence of any relationship between the protector and the settlor, and any other information or particulars relevant to the reliable and adequate verification of both the settlor and the protector in accordance with the procedures relating to the verification of client identity outlined in these directives;

d) A statement of the true purpose of the trust being established, substantiated by evidence in accordance with the procedures outlined in these Directives; and

e) A statement showing the source(s) of funds to be settled substantiated by evidence.

19.06. A Financial institution hosting a trust account shall ensure that every payment from the trust are authorized and made in accordance with the terms of the trust and in compliance with the laws of Sierra Leone.

20.00. THE REQUIREMENT FOR INTERNAL MANAGEMENT AND CONTROL MECHANISMS

20.01 Every financial institution shall have in place control mechanisms adequate to detect, prevent and report any behaviour or conduct linked to money laundering and terrorism financing.

20.02. Any measures designed by any financial institution in compliance with *para 20.01* shall be forwarded to the Unit for review and advice.

20.03. In order to ensure adequate compliance with *paras 20.01 and 20.02* every financial institution shall appoint a Compliance Officer who among other duties shall be responsible for the implementation and maintenance of reporting procedures.

20.04. A person shall not be eligible to be appointed as a compliance officer unless he is a senior officer with relevant qualifications and experience as set out in Section 35 of the Act.

20.05. Every financial institution shall upon complying with *paras 20.03 and 20.04* inform the Unit and regulatory bodies in writing about the appointment of the compliance officer annexing his certificates and any other documents relevant to his recruitment.

20.06. Every financial institution shall ensure that every member of staff at management level is regularly trained on money laundering and financing of terrorism so that they are able to deal with emerging trends in money laundering and terrorism without prejudice to any training opportunities that the financial institution may wish to offer to management staff.

20.07. The compliance officer appointed under *para 20.03* shall be responsible for the regular review of the standard reporting measures provided for under *paras 20.01 and 20.02* and the day-to-day compliance therewith.

20.08. Any suspicious transaction detected by any employee of a financial institution must be forwarded immediately to the compliance officer in the form depicted in **Appendix 4** for review and determination.

20.09. The compliance officer shall upon receipt of a report concerning a suspicious customer or transaction, determine whether the information contained in such report supports the suspicion that a customer is or could be engaged in money laundering or terrorism financing by investigating the details in order to determine whether the circumstances are sufficient to trigger a report to the Unit.

20.10. The compliance officer shall in considering his judgment under *para 20.09* take into cognizance all other relevant information available within the institution concerning the person or entity to which the suspicious transaction relates.

20.11. The compliance officer following his evaluation of an internal report forwarded to him under **para 20.08** may give instructions for further action.

20.12 Any instruction for further action given by the compliance officer under **para 20.11** shall be followed and shall not be altered without the consent of the Compliance Officer.

20.13. The Compliance Officer shall upon his conclusion that the information he received does substantiate a suspicion of money laundering, terrorism financing or any unlawful conduct or activity report the transaction immediately to the Unit stating reasons for the suspicion.

20.14 Where the compliance officer concludes that the circumstances reported to him under **para 20.08** do not substantiate a suspicion of money laundering or terrorism financing or any unlawful act or conduct, he shall record his decision not to report the transaction to the Unit as suspicious stating reasons for his conclusion.

20.15. The compliance officer and any employee of a financial institution must ensure that all communications relating to suspicious transaction and any other or further communications ancillary or incidental thereto are treated as strictly confidential.

20.16. Any internal control regime adopted by a financial institution under these Directives shall require the maintenance of a register of all reports made to the Unit.

20.17. Any register kept by a financial institution under **para 20.16** shall contain details including but not limited to the following:

- (a) The date of the report;
- (b) The person who made the report;
- (c) The person(s) to whom the report was forwarded;
- (d) A reference by which supporting evidence is identifiable; and
- (e) The receipt of acknowledgement from the Unit.

21.00. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

21.01. Every financial institution shall upon recognising that a financial transaction bears the indicia of a suspicion of being connected with money laundering, terrorism financing or any unlawful act or conduct incidental or ancillary thereto report immediately to the Unit stating the parameters based on which the suspicion is raised setting out the report in the format as depicted by **APPENDIX 5**.

21.02. The Compliance Officer appointed under **para 20.03** shall keep branch managers and other senior officers within the financial institution informed about the development on every report of a suspicious transaction.

21.03 The compliance officer appointed under *para 20.03* shall ensure that the regulatory Authority is kept informed of any development in connection with all suspicious transaction reports received by him.

22.00. CURRENCY TRANSACTION REPORT (CTR)

22.01. Every financial institution involved in any currency transaction shall if the transaction is to be conducted for or on behalf of a natural person and the transaction is worth at least Le 30,000,000, (thirty million Leones) or its equivalent in foreign currency, file a report of the transaction with the Unit in the form depicted by **APPENDIX 6**

22.02. Without prejudice to *para 22.01* where a financial institution is involved in a currency transaction for or on behalf of a corporate body and the transaction exceeds is worth at least Le 100,000,000 (one hundred million Leones) or its equivalent in foreign currency the financial institution shall file a report on the transaction with the Unit in the form depicted by **APPENDIX 6**.

22.03. Without prejudice to *paras 22.01 and 22.02* 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 Le 30,000,000 (thirty million Leones) the financial institution shall file a report on the transaction with the Unit in the form depicted by **APPENDIX 6**

22.04. Without prejudice to *paras 22.01, 22.02 and 22.03* 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 Le 100,000,000 (on hundred million Leones) the financial institution shall file a report on the transaction with the Unit in the form depicted **BY APPENDIX 6**.

23.00. FOREIGN TRANSACTION REPORT (FTR)

23.01. Every Financial institution shall file with the Unit 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.

23.02. The obligation imposed on financial institutions under *para 23.01* shall not absolve any financial institution from the obligation to report suspicious transactions to the Unit whenever they are recognised.

23.03. Reports under *para 23.02* shall be forwarded by the financial institution to the Unit in an electronic form to be followed by a hard copy of same.

23.04. Where an investigation into a suspicious transaction shall be commenced, the Unit may request an institution to keep records of every customer directly or indirectly connected with the suspicious transaction until the financial institution is instructed otherwise by the Unit.

23.05. Where a financial institution knows, ought to have known or has reasons to suspect that an investigation into a transaction is to be commenced by the Unit, other competent authority or a regulatory body the financial institution 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 the Unit.

23.06. Every Financial institution 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 the Unit or other competent authorities.

23.07. The register of enquiries contemplated by *para 23.06* 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.

23.08. Every financial institution shall ensure that every register kept and maintained under *paras 23.06 and 23.07* is preserved for at least five years.

23.09. When an investigation into a transaction linked to a register kept and maintained under *paras 23.06 and 23.07* shall be commenced by the Unit, other competent authority or regulatory body the Unit, 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 the Unit, other competent authority or regulatory body.

23.10. Where a financial institution 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 23.06 and 23.07* is to be commenced by the Unit, other competent authority or a regulatory body the financial institution shall preserve the register until otherwise instructed by the Unit other competent authority or regulatory body.

24.00. THE OBLIGATION TO KEEP RECORDS OF TRANSACTIONS

24.01. Every financial institution 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, passport and identity card numbers of customer and any other or further particulars that will facilitate the comprehensive identification and profiling of the customer.

24.02. Without prejudice to *para 24.01* a financial institution shall clearly identify any beneficial owner different from the customer directly dealing with the financial institution in the mode prescribed thereby.

24.03. A financial institution in compiling the records of a transaction 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.

24.04. Where a transaction involves securities and investment, the financial institution in compiling transaction records in compliance with *para 24.01* 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; and
- (n) Any further particulars that would facilitate the reconstruction of the transaction and analysis thereof

24.05. In dealing with transactions involving electronic transfers a financial institution 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 of the funds;
- c) The identity of the ultimate recipient;
- d) The form of instruction and authority; and
- e) Destination of the funds.

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

24.06. Where a transaction involves domestic or international credit transfer made by electronic means the financial institution 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.

24.07. Every financial institution shall ensure that all sets of data collected and maintained in compliance with these directives are kept in a readily retrievable and accessible way without prejudice to the confidentiality obligation as provided for by the Act.

24.08. A financial institution shall ensure that the records and data contemplated by *para 24.07* are kept and secured in any retrievable form including but not limited to the following:

- a) An original hard copy;
- b) Microform; or
- c) Electronic data;
- d) Any other form that would ensure the security and easy accessibility of the data

24.09. For the purposes of *paras 24.07 and 24.08* records held by third parties shall not be regarded as being in a readily accessible and retrievable form unless the financial institution is reasonably satisfied that the third party is itself an institution which is able and willing to keep such records and disclose them to the financial institution when required.

24.10. Every financial institution shall ensure that all records and data kept and, maintained under *paras 24.07 and 24.08* are preserved for a period not less than 5 years following the end of business relationship.

24.11. It shall be mandatory for any financial institution to forward any record or data kept and maintained under these directives to the Unit upon request.

24.12 For the purposes of *para 24.10* and any business relationship that has not been formalized the five year period shall start on the date of completion of that last transaction.

24.13. Every Financial institution receiving payments for or on behalf of the National Revenue Authority (hereinafter referred to as "**THE AUTHORITY**") shall keep records containing full details of transactions thereof and submit to the Unit on weekly basis reports containing such details including but not limited to the receipts and postings undertaken, carried out or facilitated by the financial institution for or on behalf of the Authority and

any further particulars that would aid the reconstruction of every transaction contemplated by this paragraph.

Provided that a financial institution complying with this paragraph shall be at liberty to set out its own format for the purpose thereof and shall ensure that any format designed for the purpose of compliance under this paragraph shall contain such data as would meet the information need of the Unit within the spirit and intendment of these Directives.

25.00. THE OBLIGATION TO FREEZE ASSETS OF DESIGNATED PERSONS AND ENTITIES

25.01. Without prejudice to any provision contained in the Terrorism Prevention Regulations 2013, every financial institution shall maintain updated lists of persons and entities designated as being affiliated or linked to terrorism or terrorist financing by the Sanctions Committee pursuant to a UNSCR, the regional body of ECOWAS or the government of Sierra Leone.

25.02. Every financial institution shall prior to commencing or deciding to continue a business relationship with a customer screen the actual or potential customer and satisfy itself that the customer is not on a designated List.

25.03. Where a financial institution shall discover a match between the name of its actual or potential customer and that of a designated person by virtue of a list of designated persons and entities under *para 25.01 or para 25.02* the financial institution shall suspend the business relationship and refer same to the CISU for clarification without prejudice to the obligation to submit suspicious transaction reports to the Unit.

25.04. A financial institution shall in carrying out their CDD procedure under these directives make reference to every list of designated persons under these directives and shall prevent any person or entity properly so designated from entering any relationship with the financial institution or using any of their facilities or product to carry out or conduct any transaction whatsoever.

25.05. Without prejudice to *para 25.04* every financial institution shall be under an obligation to conduct ongoing due diligence with reference to every updated list of designated persons and entities to determine whether any of their customers has been designated in a manner contemplated by these directives.

25.06. Where a financial institution confirms that a customer has been designated in a manner contemplated by these directives the financial institution shall freeze every asset it holds for that customer until otherwise directed by the Unit, CISU or the Terrorism Prevention Committee.

25.07. The Director may upon receipt of list of persons or entities designated as being involved in or connected with acts of terrorism or terrorism financing institute preventive measures and instruct every financial institution having business relations with any person or entity so designated by any feasible means of communication to freeze the assets of the designated person or entity.

25.08. A financial institution shall upon receipt of instructions by the Director under *para 25.07* comply fully without delay.

25.09. Any asset(s) frozen under these directives shall not be unfrozen until otherwise directed by the Unit or other competent authority.

26.00. MISCELLANEOUS PROVISIONS

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

26.02. The Unit may, in consultation with the supervisory authorities amend and or replace any or all of these Directives and Guidelines in response to changes in the operational dynamics of financial institutions or changes in the trends of money laundering and terrorism financing.

26.03. The Anti-Money Laundering Guidelines issued to Financial Institutions by the Unit in March 2009 are hereby repealed and replaced.

26.04. These Directives and Guidelines shall be complementary to the Act and relative provisions in other enactments and therefore shall not be construed as a substitute for the Act and other related legislations.

26.05. Where there is a conflict between the Act or any other legislation in force and these Directives and Guidelines the Act or other legislation in force shall prevail.

26.06. Without prejudice to the general obligations under these directives the Unit shall be at liberty to issue other or further directives, amend or repeal any paragraph of these directives as the evolving operational circumstances in the financial system or the Unit may dictate.

26.07 Any other or further directives issued or amendment made under *para 26.06* shall be binding on every financial institution until further amended or repealed by the Unit in accordance with these directives

26.08 Any failure to comply with these Directives and Guidelines shall be punishable in accordance with Section 53 (2) and (3) of the Act and PART XI of the Terrorism Prevention (Freezing of International Terrorist Funds and Other Related Measures) Regulations 2013.

APPENDICES

APPENDIX 1

PARTICULARS NECESSARY FOR THE VERIFICATION OF INDIVIDUALS APPLYING TO A FINANCIAL INSTITUTION FOR BUSINESS

- a) Full name(s) used including nick names and aliases (if any)
- b) Date and place of birth to be supported by birth certificates
- c) Nationality (indication should be made if dual citizenship is maintained);
- d) Current permanent residential address including postal code (if applicable);
- e) Telephone, fax number and email address;
- f) Valid photo-bearing identification with unique identifier, (eg. Passport, NASSIT card, national identity card or driver's licence);
- g) Occupation and name of employer (if self employed, the nature of the self-employment);
- h) Specimen signature of the verification subject;
- i) Credit cards,
- k) Business cards and
- l) Student union cards shall not be accepted uncritically.

APPENDIX 2

PARTICULARS REQUIRED IN AN IDENTIFICATION PROCESS INVOLVING LOCAL RELIABLE INTRODUCTION

Name and address of introducer _____

Fax & Email address of Introducer _____

Telephone number of Introducer _____

Name of applicant for business: _____

Address of applicant for business: _____

Telephone Number of applicant for business: _____

Email address of applicant for business: _____

Fax Number of applicant for business: _____

The Introducer must fill the following:

1. We are an institution regulated by [name of regulatory body] in [country].
2. We are providing this information in accordance with *para 13.10(d)* of the directives.
3. The Applicant for business is/ was an existing customer of ours as at {date}

OR

4. We have completed the verification of the applicant for business and his/her name and address as set out at the head of this introduction corresponds with our records.

AND

5. The Applicant for business applying on his own behalf and not as nominee, trustee or agent.

OR

6. The Applicant for business is acting as nominee/ trustee/ in a fiduciary capacity for other persons whose identities had been established by us and appropriate documentary evidence to verify same is held by us and can be produced when required

ALTERNATIVELY

7. We have not completed the identification and verification of the Applicant for business for the following reasons.....

CONFIDENTIALITY

The above information is given in strict confidence for your own use only and without any guarantee, responsibility or liability on the part of the institution or its officials in the Event of a breach of confidentiality.

CERTIFICATION

I hereby certify that the information given above is true and accurate to the best of my knowledge, information and belief.

SIGNATURE.....

DATE.....

APPENDIX 3

FORMAT OF REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY

To: [Address of financial Institution to which request is sent]

From: [Address of Financial institution sending the request]

Dear Sir

REQUEST FOR VERIFICATION

In accordance with the Directives of the Financial Intelligence Unit, Sierra Leone we write to request your verification of the identity of our prospective customer detailed below: -

Full name of customer: _____

Title (Mr/Mrs/Ms) specify _____

Address including postcode _____

(as given by customer):

Date of birth: _____ Account No _____

Specimen of customer's signature: _____

Please respond positively and promptly by returning the torn-off portion below.

.....

.....

To: The Manager (originating branch) from: (Receiving Institution)

Request for verification of the identity of [title and full name of customer]

With reference to your enquiry dated _____ we:

1. Confirm that the above customer is/is not known to us.
2. Confirm/cannot confirm the address shown in your enquiry.
3. Confirm/cannot confirm that the signature reproduced in your enquiry appears to be that of the above customer.

The above information is given in strict confidence for your own use only and without any guarantee or responsibility on the part of this institution or its officials.

FULL NAME.....

DESIGNATION.....

SIGNATURE.....

DATE.....

APPENDIX 4

INTERNAL REPORT FORM REGARDING SUSPICIOUS TRANSACTIONS

NAME OF CUSTOMER/PROSPECTIVE CUSTOMER:	
FULL ACCOUNT NAME(S):	
ACCOUNT NO.(S)	
DATE(S) OF OPENING	DATE OF CUSTOMER'S BIRTH: DD____/MM____/YY____
PASSPORT NUMBER:	
IDENTIFICATION AND REFERENCES:	
CUSTOMER'S ADDRESS:	
DETAILS OF TRANSACTIONS AROUSING SUSPICION:	
As relevant:	
Amount (Currency) _____	Date of Receipt _____
Sources of Funds:	
Other Relevant Information:	
Name and Position of Employee making Report: _____	
Signature _____	Date: _____
Compliance Officer:	
(The Compliance Officer shall briefly set out the reason for regarding the transactions to be reported as suspicious or, if he decides against reporting, his reasons for that decision.)	
Signature of Compliance Officer _____ Date: _____	
Senior Management Approval:	
Name of Senior Manager _____	
Approved/Rejected _____	Date: _____
REASONS:	
DATE REPORT MADE TO AUTHORITY (if appropriate):	

APPENDIX 5

FORMAT OF SUSPICIOUS TRANSACTION REPORT FROM REPORTING ENTITIES TO THE UNIT

COMPLETE AS APPROPRIATE – EITHER TYPE OR PRINT FORM

1. Tick as appropriate:

(a) Confirmation of Telephone Report (b) Initial Report (c) Supplemental Report (d) Corrected Report

REPORTING ENTITY INFORMATION

2. Name		
3. Address		
	4. Telephone number	5. Fax number

PARTICULARS OF SUSPECT

7. Name (full name of person, business or company)	
8. Address	
	9. Date of Birth (DD/MM/YY)
10. Occupation	11. Employer
12. Telephone number - business	13. Telephone number – residence
14. Form(s) of identification produced by suspect	
15. Suspect's relationship with Reporting Entity	
16. Is suspect employed by Reporting Entity? (YES/NO (If "Yes" give details)	
17. Other relevant information (please include details of identification and/or references taken, associated parties, addresses, telephone numbers etc.)	
18. If this report is linked to other reports, please provide details:	

PATRICULARS OF COMPLAINT

19. Reasons for Suspicion

20. Signed by [name of person compiling report]	21. Countersigned by Money Laundering Compliance Officer
---	--

22. Telephone Number	23. Fax number	24. Telephone Number	25. Fax number
----------------------	----------------	----------------------	----------------

The Director Financial Intelligence Unit 43 Wellington Street Freetown Sierra Leone

TRANSACTION COMPLETED

☐ Y

☐ N

NOTE-When submitting this report please append any additional materials that you may consider suitable and which may be of assistance to the recipient including but not limited to bank statements, vouchers, international transfers, inter-account transfers, telegraphic transfers, details of associated Accounts etc.

APPENDIX 6

REPORTING OF CURRENCY TRANSACTION IN AMOUNTS EQUAL TO OR GREATER THAN LE 30,000,000 LMILLION (IN RELATION TO NATURAL PERSONS) OR EQUAL TO OR GREATER THAN LE100, 000,000 IN RELATION TO LEGAL PERSONS.

Reporting Entity Information

Name.....

Address.....

Telephone Number.....

Fax Number.....

Email address.....

Particulars of Customer

Name (Full name of person, business or company)

Address ----- Email ----- Tel No ----- Fax No -----

Amount

Nature and purpose of transaction

Date of transaction.....

Destination of transaction.....

Particulars of beneficiary

Name

Residential Address

c) Email address

d) Tel number

e) Fax number

If customer is recipient, state particulars of originator of transaction

Particulars

- a) Name of originator
- b) Residential Address of originator
- c) Email address
- d) Tel number
- e) Fax number
- f) Amount
- g) Nature and purpose of transaction
- h) Date of transaction

Signed by (Name of person compiling report)

Countersigned by Compliance officer (If different from person compiling the report)

APPENDIX 7

LIST OF UNLAWFUL ACTIVITIES CONTEMPLATED BY THESE DIRECTIVES

- a) Participation in organized criminal groups and racketeering
- b) Terrorism including terrorist financing.
- c) Trafficking in human beings and migrant smuggling
- d) Sexual exploitation in all its forms
- e) Elicit trafficking in narcotic drugs and psychotropic substances
- f) Illicit arms trafficking
- g) Illicit trafficking in stolen and other goods
- h) Corruption and bribery
- i) Fraud
- j) Counterfeiting
- k) Counterfeiting and piracy of products
- l) Environmental crimes
- m) Murder, grievous bodily harm or injury
- n) Kidnapping, illegal restraint and hostage-taking.
- o) Robbery and Simple Larceny
- p) Smuggling
- q) Extortion
- r) Forgery
- s) Piracy
- t) Insider trading and market manipulation
- u) Tax offences

Made this ^{4th} day of ^{September} 2017



MOMODU L. KARGBO

*Minister of Finance and Economic Development,
Chairman Inter-Ministerial Committee.
For and on behalf of the Financial Intelligence Unit*



AHMED B. KAMARA

*Director
Financial Intelligence Unit, Sierra Leone
For and on behalf of the Financial Intelligence Unit*