INTERNATIONAL BANK (LIBERIA) LIMITED

ANTI-MONEY LAUNDERING/ COMBATING THE FINANCING OF TERRORISM (AML/CFT) AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (WMD)

COMPLIANCE POLICY

DECEMBER 2016

APPROVING AUTHORITY

Title:	ANTI-MONEY LAUNDERING/ COMBATING THE FINANCING OF TERRORISM (AML/CFT) AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (WMD) COMPLIANCE POLICY		Volume:	1.0
From:	Compliance Department		Signature	Date
By:	Kojo G. Weeks	Compliance Manager		09/02/17
Concurrence:	Jackie Williams	Operations Manager		2/13/17
	Franklin Cole	Risk Manager		2/13/17
Approved by:	Henry F. Saamoi	Chief Executive Officer		2/10/17
	Estrada J. Bernard (Cllr.)	Chairman, Board of Directors		2/10/17

COPYRIGHT NOTICE

TABLE OF CONTENTS

1. INTRODUCTION

This policy details International Bank (Liberia) Limited's policy directed towards ensuring the effective implementation of various measures against Money Laundering, Terrorist Financing, the Proliferation of Weapons of Mass Destruction and other risks posed to the integrity of the financial system. The policy also provides guidance for all employees in accordance with obligations of detecting and preventing the money laundering and terrorist financing as well as ensuring that suspicious transaction/activities are identified and reported thereby protecting the bank from being used for illegal purposes. Full adherence on the part of all employees is a must as required by provisions of the CBL AML/CFT Regulation 2013 and FIU Act 2012.

i. SCOPE OF THE POLICY

This Policy applies to all employees of International Bank (Liberia) Limited (IBLL). The Policy sets out the procedures which must be followed to enable the Bank (IBLL) comply with relevant regulations, guidelines, legislation and other obligations.

Failure to comply with this AML/CFT Policy and other policies and manuals may lead to disciplinary action being taken against said employee(s) who risks the bank's reputation.

ii. PURPOSE

This Policy is intended to enable International Bank (Liberia) Limited meet its compliance requirements and appropriate internal controls in a way which is proportionate to the low risk nature of the business type and the higher risk level of the types of jurisdictions that it operates in.

To set out this AML/CFT policy all employees should be aware of the fast growing crimes of money laundering and terrorist financing, their responsibilities regarding these crimes, and the consequences of non-compliance with this policy.

Potentially any employee could be caught by the money laundering provisions if they suspect money laundering and either become involved with it in some way and/or do nothing about it. The bank remains committed to providing internal guidance and training where employees become familiar with their legal responsibilities to safe guide

individuals or the Bank from falling victim to money laundering or terrorist financing offenses.

This document is to provide an overall understanding of the money laundering and terrorist financing phenomenon and to set out policies and procedures designed to enable employees comply with statutory and supervisory policies relating to money laundering and terrorist financing.

iii. DEFINITION OF KEY TERMS

Money Laundering - is the process by which launderers attempt to conceal or disguise the true nature, location, source, ownership or control of illegally obtained money. The phrase "money laundering" or AML laws cover all methods used to change the identity of illegally obtained money so that it can be used for legitimate purposes. Money laundering is a crime derived from an initial crime referred to as predicated offences. There are twenty one (21) money laundering predicated offences (detailed in appendix 1) which includes proceeds from criminal activities such as drug trafficking, armed robbery, tax evasion, terrorism, arms dealing, fraud, forgery and counterfeiting, bribery and corruption.

Terrorist financing - refers to the processing of funds to sponsor or facilitate terrorist activity. A terrorist group, like any other criminal organization, builds and maintains an infrastructure to facilitate the development of sources of funding, to channel those funds to the providers of materials and or services to the organization, and, possibly, to launder the funds used in financing the terrorist activity or resulting from that same activity. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as drug trade, weapons smuggling and other goods, fraud, kidnapping and extortion.

Financing of the proliferation of Weapons of Mass destruction (WMD) - Financing of the proliferation of weapons of mass destruction refers to the processing of funds for the purpose of financing the proliferation of WMDs. FATF recently recommended that countries and FIs take steps to combat the financing of the proliferation of WMDs.

Financial Action Task Force (FATF) - FATF is an intergovernmental body that sets the global standards for Anti-money laundering laws and practices. It presently has 34

members, largely the world's richest countries. Though FATF has no legal enforcement powers, non-adherence to its recommendations (FTAF 40 recommendations) has far reaching effect on countries' risk rating and ability to conduct international financial transactions, hence most countries tries to implement the recommendations.

Inter-governmental Action group against Money laundering in West Africa (GIABA) - GIABA is the institution of the Economic Community of West African States (ECOWAS) responsible for facilitating the adoption and implementation of Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) in West Africa. It is also the FATF Styled Regional Body (FSRB) in West Africa and works with states in the region to ensure compliance with international AML/CFT standards.

Financial Intelligence Unit of Liberia (FIUL) - The FIUL was established April 30, 2013 by an act of national legislature which serves as the central, national agency of Liberia responsible for receiving, requesting, and conducting preliminary investigations, analyzing and disseminating information concerning suspected proceeds of crime and terrorist property. The FIUL achieves its objectives through coordination with all stakeholders including the central Bank of Liberia, law enforcement agencies, reporting entities and partners.

2. POLICY STATEMENT

International Bank (Liberia) Limited, as a commercial bank, subscribes to established laws, regulations, directives and other international laws guiding the financial industry in order to protect its good name and reputation, decrease the likelihood of becoming a victim of fraud or illegal activity and ensure safe, sound and best business practices in the financial sector.

In keeping with IBLL Mission, Values and policies, we strictly observe international laws and refuse to aid those attempting to evade them. The Bank is committed to the prevention and detection of money laundering and financing of terrorism/proliferation of weapons of mass destruction by conforming to relevant laws, regulations, standards and best practices through the adoption of a risk-based approach for the implementation of its AML/CFT policies and programs. Customers shall therefore be profiled and classified according to individual risk which seeks to guide the level of due diligence to be performed for the business relationship and/or transactions monitoring.

Staff knowledge of the information contained in this policy will help prevent the bank from being victimized by money launderers. It will also aid law enforcement officers in their efforts to track criminals and people who laundered money.

Whilst the Bank remains committed to ensuring that customers information are kept confidential, such commitment shall be in accordance with the Financial Institution Secrecy Laws whereby it shall in no way inhibit the implementation of FATF Recommendation, national or international laws.

3. STAKEHOLDERS' ROLES AND RESPONSIBILITIES

i. BOARD OF DIRECTORS

The Committee on banking supervision of Basel has mentioned that compliance starts at the top. It is most effective in a corporate culture that emphasizes standards of honesty and integrity and in which the Board of Directors and Senior Management lead by example. It concerns everyone within the bank and should be viewed as an integral part of the bank's business activities. It goes on to say that "A bank should hold itself to high standards when carrying on business, and at all times strive to observe the spirit as well as the letter of the law".

The Board of Directors remains the apex authority of the bank in the fight against money laundering, financing of terrorism and other forms of illicit activities. Upon recommendation from its sub-committee, the Board shall approve the AML/CFT compliance annual plan and ensure implementation by Senior Management.

ii. SENIOR MANAGEMENT/RISK MANAGEMENT COMMITTEE

Management through the relevant units and risk committee shall identify and mitigate various AML/CFT risks to which the bank might be exposed by ensuring that all staff remain committed to full compliance in their individual responsibilities.

Management through the compliance department shall effectively communicate to all staff and ensure adequate training in AML/CFT, KYC, CDD, reporting requirements and utilize suitable forms of testing to ensure proper understanding of the AML/CFT policies and issues.

It shall also ensure the provision of relevant tools and adequate support to staff in ensuring the implementation of an effective AML/CFT regime.

iii. COMPLIANCE MANAGER/COMPLIANCE DEPARTMENT

The compliance Manager shall be a staff designate at management level and shall be responsible for the implementation of and ongoing compliance to AML/CFT obligations of the bank. The compliance department shall have ready access to all books and records.

The Compliance Manager/Department shall review and update the AML Compliance Program as necessary due to changes in laws or regulations and ensuring that all affected employees are being advised of the changes.

The Unit shall also provide AML/CFT training to all employees on an annual basis, and shall maintain copies of, and make available to the CBL upon request, all training attendance records, training programs and materials in accordance with section 2.10 of the CBL AML/CFT regulation 2013.

Implement internal audit arrangements to review and monitor effectiveness of AML/CFT policies, procedures, systems and compliance, as well as initiate corrective actions where compliance deficiencies are identified and cooperate with law enforcement, correspondent relationships, MoneyGram/Western Union AML reviews, audits and investigations.

iv. Business Units/Processors/Managers/Compliance Champions

International Bank (Liberia) Limited shall ensure that staff are guided by relevant procedures and controls while conducting transactions so as to protect the bank from reputational risks and sanctions from regulators.

Conduct appropriate due diligence on customers and their transactions. Where applicable, take steps to establish the beneficial owners of accounts/transactions and provide feedback to the Compliance department.

Copies of this policy must be retained in relevant departments for staff review in case of doubt with a particular transaction; and

The bank encourages every staff to pay special attention to all complex transactions and promptly notify senior level staff for further validation/review and shall ensure

anonymity and confidentiality of person (s) who may whistle blow on suspicious transactions (if even it involves employee (s) of the bank and conduct validation through compliance Officer);
Failure of any staff to notify higher level officer on proven suspicious transactions, punitive administrative action (s) (fine, suspension, jail, dismissal) shall be meted where applicable.

v. All Employees

All employees of the bank has a responsibility to ensure compliance and it is as such required that they pay keen attention to possibilities of money laundering, financing of terrorism and other forms of illicit activities. Employees are to comply fully with all anti-money laundering and combating terrorist financing procedures with respect to customer identification, account monitoring, record keeping and reporting.

They are to promptly report to the Compliance department any knowledge or suspicion of money laundering/terrorist financing or where there are reasonable grounds to know or suspect.

An employee who commits ML/FT Compliance offenses shall bare the full responsibility of their actions or inactions in line with the Bank's sanction grid and provisions under the laws. All employees are strongly warned against customers being "**tipped off**" that suspicious transaction report is being or has been filed on their accounts or that their transactions are under investigation as such offense is a crime punishable as a first degree felony as provided in Article 15.8 of the AML/CFT Act 2012.

vi. Audit/Independent Review

An audit/ independent review function is responsible for assessment/testing the adequacy of the policies, procedures and practices of AML/CFT Compliance at IBLL. Recommendations from said review or audit shall be acted upon by management to ensure a timely resolution of issues raised by the Auditors (internal or external).

4. CUSTOMERS DUE DILIGENCE

The Bank remains committed to undertaking careful measures aimed at ensuring that Customers Due Diligence (CDD) is fully implemented. Significant steps are taken to ensure compliance to KYC requirements in Verifying customer's information provided at the point of boarding and beyond.

The Bank prohibits the establishment of anonymous accounts or obviously fictitious account names.

Reasonable steps shall be taken to identify each the customer and verifying the reliability/validity of the customer's information as contained in documents provided at the point of onboarding. Reliance shall also be of independent source documents, data or information from competent third party authorities.

Steps also shall be taken to identify beneficial owners of accounts in terms of understanding the ownership and control structure, purpose and intended nature of the business relationship.

The Bank shall also conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Bank's knowledge of the customer, their business and risk profile.

i. Customer Acceptance Criteria

The bank shall employ a risk based approach in signing on each new customer or in rendering service to each client. It shall apply simplified CDD measures where the risks of ML/TF are lower. Such includes the frequency of customer identification updates, limited basic requirements, etc. Where suspicion of ML/TF or specific higher-risk scenario arises, such account shall be subjected to an enhanced due diligence process.

Specific attention shall be given to Politically Exposed Persons (PEPs) and Designated Non-Financial Businesses and Profession (DNFBPs), Money Service Businesses, Casinos, Real Estate Agents, Dealers in precious metals, Lawyers, Notaries, Gambling industry, etc. based on the vulnerabilities of these categories of customers to ML/TF.

The Bank shall ensure compliance to FATF Customer Due Diligence measures as contained Recommendation 10 as a minimum standard to be followed in establishing or maintaining customer relationship:
(a) Identifying the customer and verifying that customer's identity based on reliable, independent source documents, data or information.
(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the Bank has reasonable comfort that beneficial owner is known.
(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Bank's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

During an account opening process, identification is a requirement that must not be waived by any processor/employee. Identity can be described as a set of attributes, including names used, date of birth (though information need not be verified), physical features, and the residential address at which a customer may be located, all of which can uniquely identify a natural or legal person.

ii. POLITICALLY EXPOSED PERSONS (PEPs)

Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public functions both in foreign countries as well as in Liberia. Examples of PEPs include, but are not limited to;

Heads of State of government; Superintendents; Commissioners; Senior politicians; Senior government officials; Judicial or military officials; Senior executives of state owned corporations; Important political party officials; Family members or close associates of PEPs; and Members of Royal Families.

Senior management approval shall be obtained before establishing business relationships with PEPs.

In addition to performing CDD measures, the Bank has put in place appropriate risk management systems to determine whether a potential customer or existing customer or the beneficial-owner is a politically exposed person.

For detailed information, see "Process Manual for monitoring Politically Exposed Persons (PEPs)".

iii. Prohibitions

The Bank prohibits individuals maintaining account(s) under "ANONYMOUS" or "FALSE" names. The bank also prohibits establishing relationship with entities otherwise known as "SHELL ENTITIES" with no physical presence in Liberia or country of incorporation.

All individuals and entities designated on the UN Sanction, OFAC, EU, AU, etc. are prohibited from establishing or continuing relationship with the Bank. In the event where a customer already onboard becomes designated by a competent authority, the bank shall take appropriate measures (reporting, restricting, closure, etc.) as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

iv. Account opening requirements

The Bank shall ensure that all relevant parties to establishing a transactional (banking) relationship have been sufficiently identified and the nature of the business they intend to conduct ascertained. That is, account opening procedures as clearly spelt out in the Banking Operations Manual which entails what information a prospective customer should provide. This information is to be obtained by the designated officer opening an account for the applicant and they are to specifically ensuring that KYC requirements are fully complied with.

For the establishment of business relationship with a new customer, the below minimum documentation requirements shall be met:

A. REQUIREMENTS FOR PERSONAL ACCOUNTS HOLDERS

1. Two resent passport size photos
2. Valid Identification (Passport, Driver's License, Government issued IDs)
3. Residence Permit (In case of a FOREIGNER)

B. BUSINESS (IN ADDITION TO REQUIREMENTS INDICATED IN A. FOR EACH SIGNATORIES)

1. Business registration Documents
2. Corporate / Board resolution
3. Articles of incorporation
4. Letters of Administration/Authority (If Applicable)
5. Partnership Agreement
6. By-Laws
7. Power if Attorney (If Applicable)
8. Reference

C. NGO/INGO (IN ADDITION TO REQUIREMENTS INDICATED IN A. FOR EACH SIGNATORIES)

1. Power/letter of authority
2. Letter of accreditation
3. Article of incorporation
4. By-Laws and constitution (probated and notarized)
5. Business registration
6. Board Resolution

v. Transactional (Deposits, Withdrawals, Wires/Remittance) services

The Bank seeks to ensure the prevention and detection of misuse of its facilities or services by terrorists and other criminals from having unrestricted access to wire transfers/remittances for moving their funds. Reasonable steps shall be taken to enhance the minimum requirements by FATF standard to ensure that the Bank has satisfactory information on both the remitter and beneficiary of any transfer:

(i) Name, address, identification and other details of remitter;
(ii) Name, address, identification and other details beneficiary;
(iii) Account number for each, or a unique transaction reference number;
(iv) Source of fund; and
(v) Purpose of transfer.

Where there exists suspicion of money laundering or terrorist financing the Bank shall take reasonable steps to verify the information relative to its customer. Such suspicion shall be filed with the competent authority, the FIU via a Suspicious Transaction Report (STR). It is therefore mandatory that all wires (out-going and In-coming) meet the standard of having required and accurate information for easy filing as provided in the sections earlier mentioned.

5. MONITORING REGIME

The Bank shall monitor transactions for detection of unusual/suspicious items. The Compliance department shall monitor and ensure that procedures in place to identify clients at inception of relationship; accounts opening, deposits, withdrawals, transfers, purchases of Letter of Credits (LCs) and Manager Checks (MCs) are strictly adhered.

The Bank shall ensure that anonymous accounts are identified and purged out of the system.

Procedures and controls shall be communicated, assessed and enforced effectively by the Internal Audit, Risk and Compliance Staff.

The Bank shall maintain an effective and efficient control system including:
Know your Customers (KYC) and Customer Due Diligence (CDD) rules and suspicious transactions.

Monitoring shall seek to ensure reporting to counter the incidence of financial crime through the Bank for internal discipline and strict enforced.

The bank has integrated in its SWIFT platform the Fircosoft Screening Software powered by Bankserv Africa for effective monitoring by Treasury. Fircosoft is the recognized market leader of watch list filtering solutions, and is part of Accuity, the leading provider of global payment routing data and anti-money laundering solutions to banks and businesses worldwide. The Bank has engaged the services as additional control measure for all incoming and outgoing remittances to be at all times subject to screening through the Fircosoft Screening Software.

The Bank shall also aspire to ensure the automation of its monitoring regime through the acquisition of additional software and enhance monitoring parameters of the core banking software for transaction screening and reporting.

6. MANDATORY DISCLOSURIES – CTR & STR

i. Currency Transaction Reporting (CTR)

The Bank shall ensure compliance to the mandatory filing of Currency Transaction Reports (CTRs) through its Compliance Department as a means of preventing and

detecting money laundering and terrorist financing, as well as enhance integrity of the financial system.

Currency Transaction for the purpose of this policy includes currency deposits, withdrawals, foreign exchange, purchase of monetary instruments with currency, or any other transaction which causes an exchange of currency between the bank and a client.

The Bank shall file consolidated CTR for each day to the FIU no later than Three (3) working days after the occurrence of the transaction for which the CTR is being filed pursuant to Section 3 of the FIU Act. If a currency transaction also qualifies as suspicious transaction, both CTR and Suspicious Transaction Report (STR) shall be filed.

This is applicable to transactions in Liberian dollars (LRD), United States dollars (USD) and the USD equivalent of currency transaction denominated in other currencies as stipulated in the table below:

USD	**LRD**	**Type of Customer**
5,000 & above	*100,000 & above*	Individuals
10,000 & above	*1,000,000 & above*	Businesses & Institutions

Guidance in given by the FIU that in order to determine whether the threshold trigger is met, where there is more than one transaction, the following shall apply:

(a) currency transactions at a single entity means transaction from all branches made to or on behalf of a single entity or account holder shall be accumulated and treated as one transaction provided that all such transactions occurred within 24 hours;
(b) currency transactions to any particular account, irrespective of who made the deposits or withdrawals, or in what installments, provided that all such transactions, when aggregated, meet the threshold above and provided also that same occurred within 24 hours;

(c) all transactions which are structured in such a manner as to put a reasonable person on notice that the person or institution involved is evading or attempting to evade the CTR threshold and by so doing avoiding a CTR filing (*FIU/CBL/SR1A-CTR/02/2016)*.

* here is no exemption in filing of CTRs on any customer, individual or corporation local or international.

Non-Compliance – the Bank could be deemed to be non-compliant to the FIU regulation and could be sanction for violation if it:
a) files CTR late; meaning the bank files the CTR beyond the statutory 3 working days period;

b) fails to abide by the FIU stipulated procedure and format for filing;

c) unlawful exemption; and

d) declines to file CTR or omits accounts or mandatory fields or sections

Staff shall be sanctioned individually or jointly if found liable for the Bank being deemed Non-compliant by the regulator. The penalty for individual or joint action or inaction shall range from warning to dismissal depended on applicable sanction levied against the bank as spelled out in Section 3.2 of the CTR Regulation of the FIU.

ii. Suspicious Transaction Reporting (STR)

Suspicious transaction is defined as any transaction thought for any justified reason that is related to the proceeds of any crime or related to money laundering or terrorist financing (Section 1.4 a of FIU STR Regulation 2016) A transaction which involves unjustifiable frequency, deliberate splitting to avoid meeting reportable thresholds, unusual complexity, conditions with no economic or lawful objective, potential fraud or which from the perspective of the Bank is contrasting with the account/customer profile.

By regulatory requirement, the Bank shall file suspicious transaction reports in accordance with FATF 40 Recommendation (R.20). The process of reporting suspicious transaction can be initiated by any staff of the bank and it's the responsibility of the Compliance Unit to file the reviewed STRs to the regulatory agency.

* For additional details, see "Procedural Manuel for Suspicious Transaction Reporting"

7. RECORD KEPPING REQUIREMENT

IBLL Ensures that existing customers' information is updated regularly, any change in previous information; it should be urgently validated;

Records keeping shall be stored in a manner retrievable for as long as the bank is in existence;

The Bank shall maintain all records of transaction, both domestic and international, for at least five (5) years following completion of transaction or longer (if requested by the CBL in specific cases). This requirement applies regardless of whether the account or business relationship is ongoing or has been terminated; and Note that false information given and not validated is used by criminals to launder their money through unwitting financial institutions.

8. EMPLOYEE TRAINING

The Bank shall seek to ensure that all employees are aware of the laws governing AML/CFT through the provision of periodic trainings. The Compliance department shall provide AML/CFT training to all employees at least on an annual basis. Copies of attendance record and training materials shall be properly maintained and made available to the CBL or FIU upon request for examination.

The Bank shall ensure that staff has access to relevant AML/CFT policies and materials and each staff shall also confirm receipt and understanding of policies.

9. REVIEW PROGRAM

The Bank shall ensure an annual assessment of its AML/CFT risks and take appropriate steps to plan and implement strategies aimed at addressing issues identified by said assessment process. The AML/CFT policy shall be reviewed and provisions made for update where there exists important development for amendment.

The compliance program/plan shall be reviewed and approved annually and be subject to independent review by both the Bank's Internal and External Auditors who shall issue opinions on the adequacy of controls, implementation and adherence.

Appendix – A DESIGNATED CATEGORIES OF OFFENCES

- Participation in an organized criminal group and racketeering;
- Terrorism, including terrorist financing;
- Trafficking in human beings and migrant smuggling;

- Sexual exploitation, including sexual exploitation of children;
- Illicit trafficking in narcotic drugs and psychotropic substances;
- Illicit arms trafficking;
- Illicit trafficking in stolen and other goods;
- Corruption and bribery;
- Fraud;
- Counterfeiting currency;
- Counterfeiting and piracy of products;
- Environmental crime;
- Murder, grievous bodily injury;
- Kidnapping, illegal restraint and hostage-taking;
- Robbery or theft;
- Smuggling; (including in relation to customs and excise duties and taxes);
- Tax crimes (related to direct taxes and indirect taxes);
- Extortion;
- Forgery;
- Piracy; and
- Insider trading and market manipulation.

Appendix – B SUSPICIOUS TRANSACTIONS' INDICATORS

Client conducts transactions involving countries known as narcotic source countries or as trans-shipment points for narcotics or that is known for highly secretive banking and corporate law practices.
Conducts multiple transactions with same bank at different branches over period of a day/week/month.
Conducts multiple transactions with various banks over period of a day/week/month.
Customer instructs that funds are to be picked up by a third party on behalf of the payee.
Customer performs activities for multiple nominees (or on behalf of), such as friends and family.
Customers who appear to know each other and each do a transaction close to record keeping or reporting limits.
Increase in cash activities at specific branch/location.
Multiple products purchased by same customer.
Multiple transactions completed by same customer at different locations.
Multiple transactions completed by same customer over period of a day/week/month.
Multiple transactions on the same day to the same beneficiary.
Same address/different customer transactions.
Same customer last name transactions.
Significant transactions relative to a relationship, transactions that exceed required limits (regulated threshold)
Single and multiple transactions completed just below reporting and recording thresholds.
The age, appearance and dress of the customer conflict with a transaction of that type or value.
The customer asks about your internal procedures and doesn't' start the transaction until he/she knows what they are.
The customer asks to split a transaction or conducts multiple transactions in the same currency to just under the large transaction level. This is known as 'smurf'.
The customer conducts a large encashment of Travellers Cheques that were purchased very recently, or customer is in a hurry to discount the cheque drastically and is in a hurry to receive.
The customer conducts regular or large transactions that do not appear to be travel or business related.

The customer does not know how much money they have and asks the staff member to count their cash.
The customer downsizes the transaction to just under the large transaction level.
The customer is in a hurry, aggressive or demanding.
The customer is reluctant to provide ID or the address details or has various forms of ID in different names.
The size of the transaction itself.
The transaction includes some counterfeit notes.
Transactions where payments are sent/received from 'high-risk' countries/locations.
Unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.
Very high account turnover inconsistent with the size of the balance or transactions which fall out of the regular pattern of the account's activity.

AGREEMENT AND DECLARATION

"I _____ hereby declare that I have read and understood the ANTI-MONEY LAUNDERING/ COMBATING THE FINANCING OF TERRORISM (AML/CFT) AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (WMD) COMPLIANCE POLICY which contains International Bank Liberia Limited rules and regulations, and subscribe and agree to be bound by the policy and rules, as amended from time to time.

I further declare that I shall regard as strictly confidential, and by no means, reveal to any person(s) whatsoever, any information concerning affairs of a customer unless required by this policy or by law compelled to by competent authority, or officially instructed by the Bank to do so in discharge of my duties."

Signature: _____

Name: _____

Address: _____

ID. No: _____

Date: _____