# Wapic Insurance Plc

## Policy on Anti-Money Laundering and Countering Finance of Terrorism (AML/CFT)

| | DESIGNATION | SIGNATURE | DATE |
|---|---|---|---|
| Prepared By | Head, Compliance and Internal Control | | |
| Reviewed By | Chief Risk Officer | | |

**Table of Definitions**

The table below defines the meaning of words and abbreviation as used in this document

| S/N | WORD / ABBREVIATION | MEANING |
|---|---|---|
| 1 | Wapic | Wapic Insurance Plc and its subsidiaries |
| | | |
| | | |
| | | |

**Approval Page**

| Name | Title | Signature |
|---|---|---|
| Mary Agha | Company Secretary | |
| Aigboje Aig-Imoukhuede | Board Chairman | |

## Table of Contents

## 1.0 Introduction

The most important means by which Wapic can avoid criminal exposure to customers who use the resources of the company for illicit purposes is to have a clear and concise understanding of the "customers" practices. Also, adoption of an effective "Anti-Money Laundering / Countering Finance of Terrorism (AML/CFT)" policy will enhance the company's ability to comply with relevant regulatory requirements.

## 1.2 Definition of Money Laundering and Terrorist Financing

Money laundering is a process in which assets obtained or generated by criminal activity are moved or concealed to obscure their link with the crime. Perpetrators of the crime find ways to launder the funds in order to use them without drawing the attention of authorities.

Money laundering empowers corruption and organized crime where corrupt public officials and criminals are able to launder proceeds from crimes, bribes, kick-backs, public funds and on some occasion, even development loans from international financial institutions. Organized criminal groups want to be able to launder the proceeds of drug trafficking and commodity smuggling through the financial systems without a trace. In the modern day definition, money laundering now covers various offences including child trafficking, prostitution, etc. Generally, Money laundering has three stages described below:

**Placement:** The physical disposal of cash/property derived from criminal activity. The purpose of this stage is to introduce proceeds into the traditional or non–traditional financial system without attracting attention e.g. purchase of artwork, cash deposits, casinos etc.

**Layering:** This involves separating source of proceeds from ownership by changing the form. It is designed to hamper audit trail e.g. complex wire transfers, resell of assets/properties, purchase of multiple investment-linked life policies to disguise origin of funds etc.

**Integration:** Re–channeling the laundered funds back to the financial system as legitimate funds.

The degree of sophistication and complexity in the money laundering scheme is infinite and is limited only by the creative imagination and expertise of criminals. Terrorist activities are sometimes funded from the proceeds of illegal activities.
Although often linked in legislation and regulation, terrorist financing and money laundering are conceptual opposites. Money laundering is the process where cash raised from criminal activities is made to look legitimate for re-integration into the financial system, whereas terrorist financing cares little about the source of the funds, but it is what the funds are to be used for that defines its scope.
In recent years, the international community has become more aware of the dangers that money laundering and terrorist financing poses in all these areas, and many

governments and jurisdictions including Federal Government of Nigeria have committed themselves to taking action. The United Nations and other international organizations like Financial Action Task Force (FATF) are committed to helping governments in any way they can to deal with the problem of AML/CFT. As a corporate organization, Wapic Insurance is committed to the success of AML/CFT efforts by both Nigerian government and other international organizations.

### 1.3 The Responsibility of Individual Employee of Wapic Insurance Plc

In adhering to this Policy, as with every aspect of its business, Wapic expects that its employees will conduct themselves in accordance with the highest ethical standards. Wapic also expects its employees to conduct business in accordance with applicable money laundering laws. As an employee of Wapic, it is mandatory for you to read and understand the AML/CFT Act and other relevant regulatory guidelines in respect of AML/CFT. Wapic employees shall not knowingly provide advice or other assistance to individuals who attempt to violate or avoid money laundering laws or this Policy.

Money Laundering laws apply not only to criminals who try to launder their ill-gotten gains, but also to financial institutions and their employees who participate in those transactions, if the employees know that the property is criminally derived. “Knowledge” in this regard includes the concepts of “**willful blindness**” and “conscious avoidance of knowledge”. Thus, employees of a financial institution whose suspicions are aroused, but who then deliberately fails to make further inquiries, wishing to remain ignorant, may be considered under the law to have the requisite “knowledge”.

Wapic’s employees who suspect any money laundering activities should refer the matter to the Company’s Chief Compliance Officer.

Failure to adhere to this Policy may subject Wapic insurance employees to disciplinary action up to and including termination of employment. Violations of money laundering laws also may subject erring employees to imprisonment and, together with Wapic as an entity to fines, forfeiture of assets, and other serious punishment.

### 1.4 Responsibility of the Company

Wapic Insurance Plc as a company has put AML/CFT policy in place to equip all its officers of the company with necessary information and skills to guard against signing on persons and organizations involved in money laundering and financing of terrorism.

### 1.5 Regulatory Framework

Nigerian insurance companies are monitored for compliance with anti-money laundering requirements under the provisions of various regulations which are highlighted below:

**List of Regulations**

a) Money Laundering (Prohibition) Act 1995 & 2004, 2011 as amended in 2012.
b) NAICOM Anti-Money Laundering and Countering the Finance of Terrorism Regulations, 2013
c) Advance Fee Fraud (419) Act 1995, Amended 2006.
d) Nigeria Drug Law Enforcement Agency Act 1989
e) Banks and Other Financial Institutions Act 1991 as amended
f) Failed Company Act 1996
g) Foreign Exchange Act 1995
h) Economic and Financial Crimes Commission (EFCC) Establishment Act 2004
i) Corrupt Practices and Other Related Offences Act 2000

The regulators that enforce compliance with the Acts are as shown below:

- National Insurance Commission (NAICOM)
- The Nigeria Financial Intelligence Unit (NFIU)
- Nigeria Drug Law Enforcement Agency (NDLEA)
- The Economic and Financial Crimes Commission (EFCC)
- Nigeria Deposit Insurance Corporation (NDIC)
- Central Bank of Nigeria (CBN)
- Securities and Exchange Commission (SEC)
- National Agency for Food and Drug Administration (NAFDAC)
- Corporate Affairs Commission
- Customs and Excise
- Nigerian Police

### 1.6 Compliance with Legislation

Wapic will observe high ethical standards within the confines of the laws and regulations guiding its operations. In particular, insurance companies are required to ensure full compliance with the NAICOM – issued Guidance Notes on Money Laundering Surveillance in order to enhance the effectiveness of the provisions of the Money Laundering Decree. Wapic insurance is aware of this requirement and will ensure that all its businesses comply accordingly.

### 1.7 Cooperation with Law Enforcement Authorities

Wapic will give full cooperation to law enforcement authorities within the limits of the rule governing confidentiality. For instance, where a company is aware of the facts that certain funds used in purchasing a policy or the subject matter of an insurance contract was derived from criminal activity or intention, the company is expected to observe the stipulated procedures for disclosure of suspicious transactions by reporting to the NFIU immediately. Wapic insurance is aware of

the need to cooperate with law enforcement authorities in the continuous efforts to fight money laundering and terrorist financing.

## 2.0 Objectives

The objectives of Wapic AML/CFT policy are as follows;

1.1 Ensure that Wapic is in full compliance with all statutes and regulations relating to AML/CFT and adheres to sound and recognized insurance practices.
1.2 Ensure that Wapic will not become a victim of illegal activities perpetrated by its customers.
1.3 Ensure an effective policy that protects the good name and reputation of Wapic.
1.4 Ensure that the policy does not undermine the cordial relationship between Wapic and its credible customers.

## 3.0 Scope and Contents of the Policy

This policy is applicable to Wapic Insurance Plc and its subsidiaries worldwide. The following principles will be incorporated into the business practices of Wapic and its subsidiaries both within and outside Nigeria.

### 3.1 Customer Due Diligence (CDD):

Wapic will make a reasonable effort to determine the true identity of all customers requesting the company's services. Policy booking procedures will require proper identification of every customer at the time the business relationship is established.
Wapic Insurance will take particular care to identify the ownership of all policies, especially for customers seeking to conduct significant business transactions. Wapic will put in place a process for the identification of unusual transactions and activities that are inconsistent with the customer's known business. In this regard, the company has established a set of procedures that facilitates the collation of sufficient information to develop a 'transaction profile' for each customer. The primary objective of such procedures is to enable Wapic predict with relative certainty the types of transactions in which a customer is likely to engage. Internal systems will then be developed to monitor customers' transactions with a view to determining if such transactions are inconsistent with customers' 'transaction profile'

### 3.2 Appointment of Chief Compliance Officer:

The company shall appoint a management staff as its Chief Compliance Officer

### 3.3 Suspicious Transactions Reporting and Currency Transaction Reporting:

Once identified, Wapic will report suspicious transactions immediately. And Qualifying Currency Transaction shall be reported to NFIU within seven days of the transactions.

### 3.4 AML/CFT Training:

Establish internal training programs for the company's employees and agents

### 3.5 Record Keeping:

This shall be in line with the provision of Section 7 of Money Laundering (Prohibition) Act 2011, amended 2012

### 3.6 Independent Audit of AML/CFT programme:

The Internal Audit shall carry out independent audit of the company's AML/CFT programme at least twice in a year

## 4.0 Customer Due Diligence (CDD)

In relation to AML/CFT, the intent of Customer Due Diligence is to ensure that criminals do not use Wapic as a financial institution to launder illicit wealth. So the extent of CDD and Know Your Customer (KYC) documentation requirements for transactions will be tied to the risk of money laundering or terrorist financing posed by the transactions, products, services or the customer's location. The implication of this is that transactions will be categorized either as High Risk, Medium Risk or Low Risk. The idea behind this is to ensure that sufficient energy and resources is focused on transactions with high risk of money laundering or finance of terrorism. Where a business has a very high risk of money laundering or finance of terrorism, Enhanced Due Diligence (EDD) will be carried out on the customer.

Particular care should be taken to ensure that full identification and "Know Your Customer" requirements are met if the customer is an International Business Company (IBC) registered in an offshore jurisdiction and operating out of a different jurisdiction. The details and identification of the promoters should be obtained. An enhanced due diligence applies for all customers whose risk assessment rating is categorized as High Risk.

Documents, data or information collected under the CDD process will be kept up-to-date and relevant by undertaking reviews of existing records, particularly of records in respect of high risk business relationships or customer categories.

### 4.1 Customer Risk Assessment Process

Wapic Insurance businesses will assess AML/CFT risk by classifying policies into different categories of Risk such as high, medium, and low. The policy type, the

customer, products and transaction types etc are some of the major determinants of policy risk rating. The Company uses its risk assessment framework in classifying its customers at the point of entering into the business relationship with the customer and as long as the business relationship continues. The risk consideration covers jurisdiction, products, services, nature of business, purpose of policies, age of customer, transaction types and actual/anticipated volumes or activity that will be carried out by customer, address location etc. Please see the company's AML/CFT risk rating grid in appendix 1 for guidance.

### 4.1.1 High Risk Customers

Before establishing relationship with prospective customers, the Relationship Manager (RM) or the Account Officer (AO) to the customers is responsible for carrying out a formal assessment of risk on the policy and classifying them as high, medium or low risk. High–risk policies are likely to exhibit one or more characteristics as described in the guideline below. Such High Risk Policies will be kept under close review by the RM or Account Officers and Compliance Unit. Any suspicion that policies are being used to launder the proceeds of crime or to assist the financing of terrorism will be reported to the Chief Compliance Officer or Anti Money Laundering Compliance Officer*.*

**Guidelines for the Assessment of High Risk Customers**

High-risk customers are likely to exhibit one or more of the following characteristics: *Politically/Financially Exposed Persons (PEPs/FEPs) and Non-Governmental Organisation (NGOs) (including corporate entities that are owned or controlled by such persons***)**

The Know Your Customer (KYC) and Anti Money Laundering Policy of the Company emphasize the need to exercice due diligence in booking policies or allowing transactions in the following instances:

- Politically Exposed Persons (PEPs)
- Financially Exposed Persons (FEPs)
- Non-Governmental Organisations (NGO)
- Where the sum-insured/Assured is very high
- Where the sum insured/assured is disproportionate to the insured/assured known income

Executive Management approval should be obtained by the Account Officer or the RM before such transactions are booked and it should also be reported to the Chief Compliance Officer

### 4.1.2 High Risk Geography

Care should also be taken when doing business with customers or third parties located in countries with a history of supporting terrorism; or section of a country where terrorism is active (e.g states where Boko Haram is active in Nigeria) or, bases for drug production/distribution; or suffering from civil unrest/civil war.

### 4.1.3 High Risk Products

These are majorly investment linked products where the benefit sums are very huge

### 4.1.4 Politically Exposed Persons (PEP)

A PEP is an individual who is occupying a public office or who had occupied a public office in the past, all his relations and associates as well as any individual with significant influence.

Executive Management approval should be obtained by the Account Officer before business transactions are processed for PEPs. PEPs transactions are rated high risk. Qualifying transactions must be sign-off by the SBU Group Head, approved by the SBU line ED and the MD/CEO.

Since PEPs are high risk, EDD shall be conducted on them before policies are booked for them.

## 4.2 Know Your Customer (KYC)

Know Your Customer (KYC) process has two basic stages. The first stage is gathering of information to identify the customer and the second stage is to verify the information provided by the customer. The stage 1 of KYC process can be effectively done with the use of proposal form. The stage 2 entails collection of documentary evidence to validate the information on the proposal form and verification of the documentary evidence.

On a general note, Wapic will not enter into any insurance contract with any entity (Individual or Corporate) without obtaining the minimum information required to identify the customer. At the minimum, the following customer's information should be obtained before booking any policy:

- The customer's Name
- The customer's form of ID (ID details)
- The customer's Contact Address
- The customer's source of funds
- The customer's source of income and assets

**4.2.1** In addition to ensuring that all the customers' information above are captured on the Proposal Form, the Relationship Managers or the Account Officers are required to obtain documentary evidence to confirm the validity of such information if the transaction or the customer AML/CFT risk rating is medium or high. However, the extent of CDD (verification of the information) depends on the risk rating.

**4.2.2** Wapic businesses shall have policies and procedures for obtaining and updating customers' information obtained at the time of the establishment of a relationship i.e. "customer's profile". To achieve this, customers' information shall be obtained and updated during renewal or at the time of claims payment.

**4.2.3 Information on customers of Wapic insurance subsidiaries:** Wapic insurance shall establish policies and procedures under which any of its businesses can rely upon another Wapic Insurance subsidiary for information on the identification of a customer who maintains mutual relationship

**4.2.4** Payment in respect of Life Insurance to a third party is prohibited except in cases like superannuation, gratuity accumulations or payment to a legal hier in case of death benefits or in complying with regulatory/legal requirements (e.g Pension Reform Act 2004). Please note that this exception is okay only if CDD has been conducted on the relevant third party.

### 4.3 AML/CFT Risk Rating and KYC Documentation Requirements

The criteria for AML/CFT risk rating of a transaction or policy depends on the ***Premium Paid***, ***Mode of Payment***, ***Nature of the product***, ***the customer involved*** and ***customer's location***. The AML/CFT risk rating is as shown in Appendix 1. Every officer of the company should read and be very conversant of the AML/CFT rating grid.

### 4.4 Responsibility for Ensuring Complete KYC Documentation

- Each Account Officer has the responsibility to obtained adequate and complete KYC documents for all the businesses that report to him or her based on the AML/CFT rating.
- The Underwriting Unit must ensure that the KYC documents or an approved KYC deferral form is duly executed before booking any business
- The Underwriting Unit should maintain and update KYC tracker to record the details of the businesses with outstanding KYC documents. See appendix 1 for the KYC tracker format
- Every Monday or any other first working day of the week where Monday is a public holiday, Underwriting Unit should send out the report of businesses booked with KYC deferral to the responsible Account Officers with copy to the relevant Group Heads, Compliance Unit, Internal Audit and Executive Management
- Compliance and Internal Control should review to ensure that complete KYC documents or approved KYC deferral forms are in underwriting files.
- Compliance and Internal Control should monitor the KYC tracker and do a weekly report to management on un-regularized overdue KYC documents

### 4.5 Booking Transaction without Complete KYC Documentation

Where an Account Officer brings a business without the necessary KYC, Underwriting unit can book the business with an approved KYC deferral form (See appendix 2). The table below shows level of approval required for KYC deferral

| Period of Deferral | Approval Level | |
|---|---|---|
| 7 days | GH of the Account Officer | Head of Underwriting |
| 14 Days | GH of the Account Officer | Head of Technical |
| 30 Days | GH of the Account Officer | MD/CEO |
| Extension | GH of the Account Officer | Approval authority here is the next level in the approval grid. E.g, Extension to 14 days on or before expiration of 7days requires Head of Technical sign-off. Extension to 30 days on or before the expiration of 7 or 14 days requires MD/CEO sign-off<br><br>**An additional 30 days extension can be granted with the approval of MD/CEO but the cumulative extension shall not exceed maximum of 60 days*. |

### 4.6 Failure to Regularize After the expiration of the Deferral

Where an Account Officer fails to regularize or seek for an extension of the deferral, a warning letter with a copy to his/her HR file will be issued. Where the KYC is not regularized after 60 days a warning letter with a copy to his/her HR file will be issued to the responsible RM or Account Officer. If the KYC is yet to be regularized after 60 days the responsible RM or Account Officer will lose 10 appraisal points.

### 4.7 Regularization of KYC during Claims or Cancellation

Where the KYC documents remain outstanding and the customer has filed for claims or cancellation of the policy, submission of outstanding KYC document will be among the compulsory documents which the customer must submit before the claims is paid or the cancellation is processed.

Before processing Claims or policy cancellation/surrender instruction, the Claims Officer should obtain the current KYC tracker from the Underwriting Unit and confirm that the customer does not owe any KYC document. Where the customer is owing, the missing KYC document should be listed as part of the documents required for claims payment.

### 4.8 KYC on Bancassurance Businesses

Where a bancassurance business is medium or high risk, the business can be booked without the approved KYC deferral form. However, the Bancassurance Officer should obtain copies of KYC documents from the bank and send to the Underwriting within 15 days of booking the business. The Underwriting Unit should also record the details of such business in KYC tracker to ensure monitoring and follow-up for regularization.

### 4.9 KYC on Brokers Business

For brokers businesses, where the broker fails to provide us with the KYC document, a letter will be sent to the broker asking him to confirm to us that he has conducted due diligence on the insured and he has all the relevant KYC documentation in is custody. A copy of the letter acknowledged by the broker will be kept in the file. Also, a copy of the response from the broker will be kept in the file when it is received.

### 4.10 Sanction Check

Wapic insurance shall have policies and procedures that will ensure compliance with NAICOM and standard AML/CFT global requirement for maintenance of a data base for individuals/entities subject to sanction by the United Nations in our database and render returns on any such known individuals/entities having policies in our company.

In order to ensure that we do not enter into business relationship with a sanctioned entity, the processing units are required to check every single transaction before processing for any individual/organization against this data base and report any matching details to the company's Compliance Unit. The Chief Compliance Officer will ensure that the report is submitted promptly to the appropriate regulatory authority (NFIU and NAICOM)**.** The transaction will not be put on hold until clarification is received from NFIU. The list will include OFAC List, UN List, EU List etc.

The Sanction List will be updated on a weekly basis and circularized to the processing unit

### 4.10 Customer Due Diligence (CDD) on Existing Customers

Customer Due Diligence (CDD) would be carried out on existing customers in the following circumstances:

- A transaction of significance takes place
- Customer documentation standards change substantially
- The institution becomes aware that it lacks sufficient information about an existing customer

- There is a material change in the way that the business or the policy is operated

### 5.0 The Responsibilities of Chief Compliance Officer

The company shall appoint a Senior Officer as its Chief Compliance Officer. The responsibilities of the Chief Compliance Officer include the following:

- Ensure compliance with AML/CFT requirements.
- Review and Approval of the Compliance work plan on a yearly basis.
- Ensure Compliance requirements are integrated in the day to day activities of the company and that processes are efficient and in accordance with applicable laws and policies.
- Ensure the implementation of Board decisions on Compliance matters.
- Ensure that regulatory changes are effectively implemented by the Company
- Co-ordinate and oversee the activities of the Compliance Resource Officers

### 6.0 Appointment of AML/CFT Compliance Officers for Branches

The most senior officer in the branches will serve as the AML/CFT compliance officer for the company. The AML/CFT compliance officer roles are as follows:

- Ensure that all the members of staff in the branch have adequate knowledge of AML/CFT
- Ensure that the branch complies with all the AML/CFT requirements

### 7.0 Suspicious Transaction and Currency Transaction Reporting

### 7.1 Suspicious Transaction Reporting

A suspicious transaction is a transaction which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering methods. A suspicious transaction will typically exhibit one or many of the following Red Flags. Therefore, any transaction with one or more of the red flags listed below should be reported immediately to the Chief Compliance Officer. The Chief Compliance Officer will file the STR to NFIU immediately.

- Policyholder insisting on anonymity; reluctance to provide identifying information, or providing minimal seemingly fictitious information
- Frequent Sum Assured top-ups that is done through Cash/Bank transfer involving payment of premium over and above N500, 000 per person per policy.
- Frequent policy surrenders by policy holders
- Assignment to unrelated parties without valid consideration
- Request for purchase of policy in amount considered beyond his apparent need or beyond the reach of his or her current source of income
- Buying a policy from a branch location where he does not reside or is employed
- Unusual termination of policies and calling for refund

- Frequent request for change in address
- Borrowing the maximum amount against policy soon after buying it
- Inflated or totally fraudulent claims
- Over-payment of premium with a request for a refund of the amount overpaid

Under the Terrorism (Prevention) Act 2011, amended 2012 Financial Institutions are required to file suspicious transaction report to the NFIU immediately it is discovered, where they have sufficient evidence to suspect that the funds:

a. are derived from legal or illegal sources but are intended to be used for any act of terrorism or;
b. are proceeds of crime related to terrorist financing
c. belong to a person, entity or organisation considered as terrorist

When any staff detects any "red flag" or suspicious money laundering activity or financing of terrorism, the suspicious activity should be reported to the Compliance Unit for investigation under the supervision of the Chief Compliance Officer. Every action taken on the investigation must be recorded. Wapic Insurance and its staff shall maintain confidentiality in respect of such investigation and a suspicious transaction report that may be filed with the competent authority. This action is, however, in compliance with the provisions of the money laundering law that criminalize "tipping off" (i.e. doing or saying anything that might tip off someone else that he is under suspicion of money laundering). Wapic Insurance, its directors, officers and employees (permanent and temporary) are prohibited from disclosing the fact that a report is required to be filed with the competent authorities. Tipping off may lead to dismissal of the staff involved.

Wapic Insurance will not commence business relationship or perform business transactions where customer due diligence has not been completed on customers who carryout transactions with high risk of money laundering.

When a customer fails to provide information required for a complete due diligence, the company shall not commence business relationship or shall stop business relationship if it is an existing customer. A suspicious transaction report shall be rendered to the NAICOM and NFIU in this regard.

Wapic Insurance will acquire AML and Name Filtering Solutions which are rule-based for tracking, analyzing and reporting suspicious activities and other AML/CTF alerts. Once identified, fraudulent or suspicious transactions will be reported to the appropriate regulatory authorities.

### 7.1.1 Process for Filing Suspicious Transaction

Wapic Insurance Plc conforms to both local and International regulatory requirements with respect to AML/CFT regulations. These regulations among other obligations require Wapic Insurance to file an STR (Suspicious Transaction Report) to NFIU whenever a suspicious or unusual activity is observed in respect of a customer's activity or employee of the company. This reporting requirement, if observed exonerates the company to an extent if ever the person(s) are investigated by the regulators. In

accordance with best practices, our company has been rendering suspicious transactions report where applicable to NFIU.

We have designed a suspicious transaction reporting Form as an innovative tool to help staff capture suspicious transactions companywide for effective reporting to the NFIU immediately a suspicious transaction is noticed.

**Objectives of the Suspicious Transaction Form**

- To identify unusual or fraudulent transactions
- Perform alert processing based on the rules and queues established within the application.
- Generate reports based on the types of alerts to the relevant authorities.

**Benefits**

The beauty of the suspicious transaction form is that:

- It provides first-hand information on suspicious and unusual transactions on customers' policies and employees of the company.
- It is a useful tool for transaction monitoring.
- Facilitates compliance with the regulatory requirement and affirms our ethical standard as a company.

**Responsibility**

All Processing Unit Heads, Account Officers/Relationship Managers and Compliance Unit are responsible for the use of the Suspicious Transaction Checklist.

**Functions of Users**

| S/N | FUNCTIONS | RESPONSIBILITY |
|---|---|---|
| 1 | Processing Officer | Where the processing officer is put on enquiry in respect of a customer's transactions, he should complete the STR form immediately and submit to the Unit Head for review. |
| 2 | Processing Unit Heads (Underwriting, Claims, CPU etc) | Reviews and reports suspicious transactions company wide. That is, once an unusual transaction is observed while processing a customers' request. Each Unit Head is expected to review the customer's records and file a suspicious transaction report to Compliance Unit immediately. |
| 3 | Account Officers/Relationship Managers | Reviews and reports any suspicious transaction on customer policies or activities to Compliance Unit immediately it is noticed. |
| 4 | Compliance unit | ▪ Reviews reports from Unit Heads and Account Officers/Relationship Manager to ascertain whether the customer's transaction is truly suspicious.<br>▪ Do a report to the GMD seeking |

| | | |
|---|---|---|
| | | approval for the customer to be reported to the regulatory body NFIU.<br>▪ Upon approval by the GMD, do a STR to NFIU. |

With the above structure in place, the company will be able to conveniently monitor high risk, suspicious, terrorist finance or fraudulent transactions.

**NOTE:** The customers' names that will be put on Blacklist are:

- Customers whose policies have been terminated due to irregularities with respect to KYC and nature of business.

Account Officers are to confirm review of the customer's KYC profile.
*Please see Appendix 3 for a copy of STR Form*

### 7.2 Currency Transaction Reporting

Anti-Money Laundering Cautionary Notice informing the customers of our obligation to report qualifying transaction to NFIU will be displayed in the Head Office and all the Company's branches.

The company shall report all the qualifying transactions to NFIU within seven days on NFIU GoAML portal. A qualifying transaction is any fund transfer to or from of N5 million and above for an individual and N10 million and above or for a corporate entity.

### 8.0 Staff Training

Every employee of the company, from the Janitor to the CEO shall be trained on AML/CFT at a minimum of once a year. To ensure good awareness and understanding of AML CFT, the Company shall observe the following:

a) Staff who fail to attend without genuine reason will pay N5,000 penalty
b) The supervisor of the unit with the highest attendance during the training will receive commendation letter from HR
c) AML/CFT training will be part of new hire induction program
d) Incorporate AML/CFT training as part of entry level training program

### 9.0 Countering Finance of Terrorism

Wapic Insurance shall train its entire staff to ensure that they have adequate knowledge on countering finance of terrorism. The AML/CFT training program will be designed to provide staff with sufficient knowledge to prevent the company from being used to facilitate terrorist financing as well as prevent the staff as an individual from being used to facilitate financing of terrorism. Also, the Company shall adhere to the following rules in processing transactions for any of its customers:

- Screen the customer's name against the database of sanctioned entities and individuals. This will prevent the company from dealing with terrorist and other criminals
- The company shall not transfer proceeds of insurance policy to an unknown third party
- Where a policy is procured for the benefits of a third party other than the policy holder, the identity of such beneficiary of a policy shall be confirmed before the proceeds of the policy is paid to them
- Before initiating any transfer of funds to a third party, the beneficiary's name shall be screened against the sanction list to ensure that such beneficiary is not a sanctioned entity

**10.0 Preservation of Records**

Wapic shall observe strictly the provision of Section 7 of Money Laundering (Prohibition) Act 2011, amended 2012 states that:

A financial institution shall:

- Preserve and keep records of a customer's identification of a customer for a period of at least five years after the expiration or termination of the policy or the severance of relations with the customer;
- Preserve and keep records and related information of a transaction carried out by a customer and the report provided for in section 6 of the Act for a period of at least five years after carrying out the transaction or making of the report as the case may be.

**11.0 Audit & Risk Review**

Internal Audit shall perform independent review of Compliance function twice in a year to ascertain the level of compliance with AML/CFT regulatory requirement by the company. Wapic Insurance Audit and Risk Review is another important means to protect the company and its businesses from being used by money launderers. Audit and Risk Review will evaluate Wapic Insurance businesses compliance with the Anti-Money Laundering/ Countering Finance of Terrorism Policy and all applicable AML/CFT laws.

**12.0 Document Retention**

In line with the section 22 of NAICOM's AML/CFT regulations 2013, the company shall maintain all records of transactions both domestic and international for a minimum of 5 years following completion or termination of the transaction.

Records of contracts which have been settled by claim, maturity or death, surrender or cancellation should be kept for a period of a minimum of 10 years after such settlement.

Appendix 1

## AML/CFT Risk Rating Grid

| **Customers** | **Individual** | | | **Corporate** | | |
|---|---|---|---|---|---|---|
| **Criteria** | **Low Risk** | **Medium Risk** | **High Risk** | **Low Risk** | **Medium Risk** | **High Risk** |
| Premium | < or = N200,000 | >N200,000 < N500,000 | >N500,000 | < N500,000 | >N500,000 < N1,000,000 | >N1,000,000 |
| Customers | Customers buying Life products with average annual sum assured <or= N2 million | Customers buying Life products with average annual sum assured >N2 million | All PEPs<br>Customers buying Life products with average annual sum assured >N5 million | Publicly quoted companies are low risk, hence proposal form capturing the customer's details is okay | | Corporate customers controlled by PEP buying policy with sum insured/assured > N25 million |
| Mode of payment | Cheque/Bank Transfer. Where the mode of payment is cash and the amount involved is up to N500,000.00, transaction automatically becomes High Risk irrespective of the Premium amount | | | | | |
| Products | 1. Third Party Insurance,<br>2. Bank financed transactions where the bank is the first loss payee<br>3. Child Education Plan<br>4. GIT<br>5. Personal Accident | 1. Investment Linked Life Policy with sum Assured =>N2 million but <N5 million<br>2. House Owner Home Insurance<br>3. Burglary and Housebreaking Insurance<br>4. Full Comprehensive Motor Insurance<br>5. Householder Home Ins.<br>6. Marine Hull Insurance | 1. Investment Linked Life Policy with sum assured > N5 million | 1. Third Party Insurance<br>2. Bank financed transactions where the bank is stated as the first loss payee<br>3. Fidelity Guarantee | 1. Individuals in Group Life scheme with the sum assured >5 million<br>2. Burglary and Housebreaking Insurance<br>3. Contractors' All Risk Insurance<br>4. Full Comprehensive Motor Insurance<br>5. Fire and special Perils Insurance | 1. Oil and Gas – Downstream,<br>2. Bonds<br>3. Individuals in Group Life scheme with the sum assured >N million |
| Geography | NA | NA | Where customers, third parties or the subject matter of the insurance contract is located in countries with a history of supporting terrorism; or section of a | NA | NA | Customers, third parties or the subject matter of the insurance contract is located in countries with a history of supporting terrorism; or section of a country where terrorism active (e.g states where Boko Haram is active in Nigeria) or, bases for drug |

| Customers | Individual | | | Corporate | | |
|---|---|---|---|---|---|---|
| **Criteria** | **Low Risk** | **Medium Risk** | **High Risk** | **Low Risk** | **Medium Risk** | **High Risk** |
| | | | country where terrorism active (e.g states where Boko Haram is active in Nigeria) or, bases for drug production/distribution ; or suffering from civil unrest/civil war | | | production/distribution; or suffering from civil unrest/civil war |
| Delivery Channels | Virtual or electronic delivery channels with sum Insured/assured <= N1 million | Virtual or electronic delivery channels with sum Insured/assured > N1 million | Virtual or electronic delivery channels with sum Insured/Assured > N2 million | Virtual or electronic delivery channels with sum Insured/assured <= N2 million | Virtual or electronic delivery channels with sum Insured/assured > N2 million | Virtual or electronic delivery channels with sum Insured/assured > N5 million |
| KYC Documentation | No special KYC document apart from documentation required for the purpose of underwriting the business. The Proposal Form should capture the following customer's details: Name, Place and Date of birth, Gender, Address, Tel number etc. | ID card (Any one of the following: Drivers' License, Int'l Passport, and Voters' Card) of the customer or a reference letter from somebody with valid ID with photocopy of the ID attached.<br><br>All the documentation required for the purpose of underwriting the business. The Proposal Form should capture the following customer's details: Name, Place and Date of birth, Gender, Address, Tel number etc. | ID card (Drivers' License, Int'l Passport, Voters' Card) and proof of residence. Visitation report signed by the account officer can be used in place of proof of residence.<br><br>All the documentation required for the purpose of underwriting the business. The Proposal Form should capture the following customer's details: Name, Place and Date of birth, Gender, Address, Tel number, source of funds, source of income / asset etc | No special KYC document apart from documentation required for the purpose of underwriting the business. The Proposal Form should capture the following customer's details: Name, Date of Incorporation, Address, Tel number etc | Certificate of Incorporation of the customer.<br><br>All the documentation required for the purpose of underwriting the business. The Proposal Form should capture the following customer's details: Name, Date of Incorporation, Address, Tel number, etc | Certificate of Incorporation of the customer, Form CO2 and CO7, proof of address or Visitation report signed by the account officer can be used in place of proof of address.<br><br>All the documentation required for the purpose of underwriting the business. The Proposal Form should capture the following customer's details: Name, Date of Incorporation, Address, Tel number, source of funds, source of income / asset etc |
| EDD Required? | No | No | Yes | No | No | Yes |

**Appendix 1**

KYC Tracker Template

| S/N | Policy No | Insured Name | Premium Paid | Sum Insured | List of Missing KYC Documents | AML Risk Rating | Class of Business | Source of business (Conventional or Bancassurance | Account Officer | Group Head |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |

**Appendix 2**

**KYC Deferral Approval Form**

| | | | |
|---|---|---|---|
| Name of Customer | | | |
| Class of Business | | | |
| Policy Number (*For Existing Business Only*) | | | |
| List of Documents being deferred | 1) | | 2) |
| 3) | 4) | | 5) |
| | Premium: | | AML Risk Rating (Medium or High) |
| No of Deferral Days | | Is this the first deferral? Yes ☐ No ☐ | |
| Account Officer (Name & Signature) | | If NO, state the cumulative previous days of deferral ☐ | |
| | | Reason for Deferral: | |

| **Acct Officers GH Concurrence** | **Acct Officers Line ED Concurrence** ***(Where Applicable)*** | **Approved By** |
|---|---|---|
| **Name:**<br><br>**Sign:** | **Name:**<br><br>**Sign:** | **Name:**<br><br>**Sign:** |

**Appendix 3**

**SUSPICIOUS TRANSACTION FORM**

**Date: …… Customer's Name: ……..**

**Branch/Unit: …….. Customer's Policy Number: ……**

**Date of suspicious activity: ……..**

**Total Amount Involved: …….**

**Relationship with Wapic Insurance Plc:**

Customer Contractor Employee Agent Contractor

Shareholder Director Broker Other ……..(specify)

**Narrative – Please answer the following questions to describe in detail the suspicious transaction(s):**

**Who is conducting the suspicious activity?** Include occupation, position or title within a business, the nature of the suspect's business(es) and length of relationship with the Company:

**Why do you think the transaction is suspicious?**

*Send this completed form and any supporting documentation to the Compliance Unit*

*Name*
(Not Mandatory)

*Signature and Date*
(Not Mandatory)

Appendix 4

- National Insurance Commission (NAICOM)
  Plot 1239 Ladoke Akintola Boulevard
  Garki II, Abuja
- The Nigeria Financial Intelligence Unit (NFIU)
  10, Ibrahim Taiwo Street,
  Aso Rock Villa, Abuja.
- Nigeria Drug Law Enforcement Agency (NDLEA)
  4, Shaw Road
  Ikoyi, Lagos.
- The Economic and Financial Crimes Commission (EFCC)
  Plot 1017 & 1018 Coree Bay Crescent,
  Wuse II, Abuja.
- Nigeria Deposit Insurance Corporation (NDIC)
  Plot 447/448 Constitution Avenue,
  Central Business District, Abuja.
- Central Bank of Nigeria (CBN)
  Banking Examination Department
  Tinubu Square
  Lagos.
- Securities and Exchange Commission (SEC)
  Tower 421, Constitution Avenue
  Central Business District, Garki, Abuja
- National Agency for Food and Drug Administration (NAFDAC)
  Plot 2032 Olusegun Obasanjo Way, Wuse Zone 7, Abuja
- Corporate Affairs Commission
  Plot 565, Ndola Square
  Off Michael Okpara Street
  Wuse Zone 5, Abuja
- Customs and Excise
- Nigerian Police