Extraordinary

Federal Republic of Nigeria Official Gazette

No. 14 Lagos - 1st February, 2012 Vol. 99

Government Notice No. 37

The following is published as Supplement to this *Gazette* :

Printed and Published by The Federal Government Printer, Lagos, Nigeria
FGP 07/42012/1,200 (OL 11)

Annual Subscription from 1st January, 2012 is Local : ₦15,000.00 Overseas : ₦21,500.00 [Surface Mail] ₦24,500.00 [Second Class Air Mail]. Present issue ₦1,500.00 per copy. Subscribers who wish to obtain *Gazette* after 1st January should apply to the Federal Government Printer, Lagos for amended Subscriptions.

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) REGULATIONS FOR THE INSURANCE INDUSTRY IN NIGERIA

ARRANGEMENT OF SECTIONS

SECTION :

APPENDICES

S. I. No. 7 of 2012

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) REGULATIONS FOR THE INSURANCE INDUSTRY IN NIGERIA

[30*th January* 2012] Commencement.

1.1. INTRODUCTION Introduction.

The National Insurance Commission (hereinafter referred to as NAICOM) has the primary responsibility for regulating insurance business in Nigeria and is collaborating with Nigerian Financial Intelligence Unit (NFIU) to ensure compliance with current AML/CFT legislation as it relates to the Insurance Industry.

1.2. The application of AML/CFT measures to non-depository financial institutions generally, and to the Insurance Companies in particular, has been emphasized by international regulatory agencies as a key element in combating money laundering and financing of terrorism.

1.3. Establishment of AML/CFT programs by Insurance Companies is a legal requirement in Nigeria and is consistent with international best practice as prescribed by the Financial Action Task Force (FATF), United Nations and the International Association of Insurance Supervisors (IAIS).

1.4. These regulations are therefore issued in the exercises of the powers conferred on the Commission under the Insurance Act 2003 and the National Insurance Commission Act 1997 and all other powers enabling it in that behalf to facilitate compliance with existing AML/ CFT legislations in Nigeria.

2.1. All insurance business shall be conducted in compliance with the requirements of Insurance Act 2003, National Insurance Commission Act 1997, and current AML/ CFT legislations.

2.2. The obligation to establish AML/CFT program applies to Insurance Companies only. However, each insurance company is required to integrate its Agents and Brokers into its AML/CFT programs and to monitor their compliance with its programme.

2.3. All Insurance Companies are required to state that it will comply promptly with all the requests made in pursuant to current AML/CFT legislation and provide information to NFIU.

2.3.1. Every Insurer's procedures for responding to authorized requests for information on money laundering and terrorist financing are required to meet the following :

(*i*) Prompt search of record to determine whether it has issued any policy to or has engaged in any transaction with any individual, entity, or organization named in the request ;

(*ii*) Prompt report to the NFIU, the outcome of the search ; and

(*iii*) Protecting the security and confidentiality of such requests.

2.4. Insurance Companies shall not in any way inhibit the implementation of the requirements in these regulations. Current AML/CFT Legislations have given the relevant authorities the power required to access information to properly perform their functions in combating money laundering and financing of terrorism ; the sharing of information between competent authorities, either domestically or internationally ; and the sharing of information between financial institutions, when it is required or necessary.

2.5. Insurance Companies are required to direct their employees in writing to always co-operate fully with the Regulators and law enforcement agents and to promptly report suspicious transactions to the NFIU. They are also required to make it possible for employees to report any violations of the institution's AML/CFT compliance program to the AML/CFT Chief Compliance Officer. Where the violations involve the Chief Compliance Officer, employees are required to report such to a designated higher authority like the Head of Internal audit.

2.6. Insurance companies are required to inform their employees in writing to make such report confidential and that they will be protected from victimization for making them.

2.7. Insurance Companies are required to render quarterly returns on their level of compliance to NAICOM and NFIU.

2.8. Insurance companies are required to identify, review and record other areas of potential money laundering and terrorist financing risks not covered by these regulations and report same quarterly to the Commission and NFIU.

SCOPE OF OFFENSIVE PROCEEDS

3.1. All Insurance Companies are required to identify and report to NFIU, the proceeds of crime derived from the following :

(*a*) Participation in an organized criminal group and racketeering ;
(*b*) Terrorism, including terrorist financing ;
(*c*) Trafficking in human beings and migrant smuggling ;

(*d*) Sexual exploitation, including sexual exploitation of children ;
(*e*) Illicit 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 currency ;
(*k*) Counterfeiting and piracy of products ;
(*l*) Environmental crime ;
(*m*) Murder, grievous bodily injury ;
(*n*) Kidnapping, illegal restraint and hostage-taking ;
(*o*) Robbery or theft ;
(*p*) Smuggling ;
(*q*) Extortion ;
(*r*) Forgery ;
(*s*) Piracy ; and
(*t*) Insider trading and market manipulation.

AML/CFT Institutional Policy Framework

4.0.1. In order to discharge the statutory responsibility to prevent money laundering and terrorist financing, all insurance companies should have AML/CFT program designed on a risk-based approach, which should at a minimum include the following :

(*i*) Internal policies, procedures and controls, based on the insurance company's assessment of the AML/CFT risks associated with its business, and designed to reasonably anticipate and prevent money laundering and terrorist financing.

(*ii*) Customer Due Diligence (CDD).
(*iii*) Appointment of a Chief Compliance Officer.
(*iv*) Suspicious Transactions Report (STRs) and Currency Transactions (CTRs) Report.
(*v*) On-going Employees/Agents training.
(*vi*) Record preservation.
(*vii*) Internal control/Audit.

Customer Due Diligence

5.1. Insurance companies are not permitted to establish business relationship with anonymous or fictitious policyholders.

5.1.2. Insurance companies should know the customers with whom they are dealing. The first step in setting up a system of customer due diligence is to develop clear, written and risk based client acceptance policies and

procedures, which among other things concern the types of products offered in combination with different client profiles. These policies and procedures should be built on the strategic policies of the board of directors of the insurance companies, including policies on products, markets and clients.

5.1.2. Insurance companies offering Life Insurance products should be aware that they are more vulnerable to money laundering if they sell short term coverage by means of a single premium policy than if they sell group pensions to an employer with annuities to be paid after retirement. The former is more sensitive to money laundering and therefore requires more intensive checks on the background of the client and the origin of the premium than the latter. Companies should be diligent in verifying source of wealth when dealing with requests for multiple policies to be taken out for premiums slightly below any threshold limits.

5.2. Insurance companies are required to undertake Customer Due Diligence (CDD) measures when :

(*a*) Business relations are established.

(*b*) Carrying out occasional transactions above the applicable designated premium threshold of ₦500,000.00 or as may be determined by the Commission from time to time. This includes situations where it is a single transaction or several transactions that appear to be linked.

(*c*) There is a suspicion of money laundering or terrorist financing regardless of any exemptions or thresholds that are referred to elsewhere in these regulations.

(*d*) There is doubt about the veracity or adequacy of previously obtained policyholder identification data.

Subject to 5.2 (*d*) above, insurance companies are not required (upon obtaining all necessary documents and being so satisfied) to repeatedly perform identification and verification exercise each time a customer conducts a transaction.

CUSTOMER DUE DILIGENCE MEASURES

5.3.1. Insurance companies are required to identify their customers (whether permanent or occasional, natural or legal persons, or legal arrangements) and verify the customer's identity using reliable, independently source documents, data or information (identification data).

5.3.2. All insurance companies are required to carry out the full range of the CDD measures in these Regulations. In reasonable circumstances, however, insurance companies can apply the CDD measures on a risk-sensitive basis.

5.3.3 Types of customer information to be obtained and identification data to be used to verify the information are provided as Appendix 1 to these Regulations.

5.3.4. In respect of customers that are legal persons or legal arrangements, insurance companies are required to :

(*a*) verify any person purporting to have been authorized to act on behalf of such a customer by obtaining evidence of his /her identity and verifying the identity of such a person ; and

(*b*) verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from the Corporate Affairs Commission (CAC) or similar evidence of establishment or existence, and obtain information concerning the customer's name, the names of trustees (for trusts), legal form, address, directors (for legal persons), and provisions regulating the power to bind the legal person or arrangement.

5.3.5. Insurance companies are required to identify the beneficial-owner and take reasonable measures to verify the identity of the beneficial-owner using relevant information or data obtained from a reliable source such that the insurance company is satisfied that it knows who the beneficial-owner is.

5.3.6. Insurance companies are required in respect of all customers to determine whether or not the customer is acting on behalf of another person. Where the customer is acting on behalf of another person, the insurance company is required to take reasonable steps to obtain sufficient identification-data to verify the identity of that other person.

5.3.7. Insurance companies are required to take reasonable measures in respect of customers that are legal persons or legal arrangements to :

(*a*) Understand the ownership and control structure of such a customer ; and

(*b*) Determine the natural persons that ultimately own or control the customer.

5.3.8. The natural persons include those persons who exercise ultimate and effective control over the legal person or legal arrangement. Thus :

(*a*) For companies, the natural persons are those who own the controlling interest and those who comprise the mind and management of the company ; and

(*b*) For trusts, the natural persons are the settler, the trustee and person exercising effective control of the trust and beneficiaries.

5.3.9. Where the customer or the owner of the controlling interest is a public company subject to regulatory disclosure requirements for example, a

public company listed on a recognized stock exchange, it is not necessary to identify the identity of the shareholders of such a public company.

5.3.10. Insurance companies are required to obtain information on the purpose and intended nature of the business relationship of their potential customers.

5.3.11. Insurance companies are required to conduct ongoing due diligence on the business relationship as stated above.

5.3.12. The ongoing due diligence above include scrutinizing the transactions undertaken by the customer throughout the course of the insurance company/customer relationship to ensure that the transactions being conducted are consistent with the insurance company's knowledge of the customer and/ or beneficial owner, their business, and risk profiles, including where necessary, the source of funds.

5.3.13. Insurance companies are required to ensure that documents, data or information collected under the CDD-process are kept up-to-date and relevant by undertaking reviews of existing records, particularly the record in respect of higher-risk business-relationship or customer categories.

5.3.14. The requirements for customer due diligence should apply to all new customers as well as - on the basis of materiality and risk to existing customers and/or beneficial owners. As to the latter, the insurance company should conduct due diligence at appropriate times.

5.3.15. Insurance companies must be aware that there are various transactions or 'trigger events' that could occur after the contract date and indicate where due diligence may be applicable. These trigger events include claims notification, surrender requests and policy alterations, including changes in beneficiaries.

5.3.16. Insurance company must pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose is essential to both the establishment of a business relationship and to ongoing due diligence. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help NFIU, NAICOM or other competent authorities and auditors. In this respect "transactions" should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, premium payments, requests for changes in benefits, beneficiaries, duration, etc.

ENHANCED CDD MEASURES

5.4.1. Insurance companies are required to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction. Enhanced CDD measures should apply to all higher risk business relationships, clients and transactions. This includes both high risk business relationships assessed by the insurer, based on the customer's individual risk situation, and the types of business relationships.

5.4.2. Examples of higher-risk customer categories include :

(*a*) Non-resident customers ;

(*b*) Legal persons or legal arrangements such as trusts that are personal assets-holding vehicles ;

(*c*) Companies that have nominee-shareholders or shares in bearer form ;

(*d*) Politically exposed person (PEPs).

5.4.3. with regard to enhanced due diligence, in general, the insurer should consider which of the following, or possible additional measures as appropriate :

(*a*) certification by appropriate authorities and professionals of documents presented ;

(*b*) requisition of additional documents to complement those which are otherwise required ;

(*c*) performance of due diligence on identity and background of the customer and/or beneficial owner, including the structure in the event of a corporate customer ;

(*d*) performance of due diligence on source of funds and wealth ;

(*e*) obtaining senior management approval for establishing business relationship ;

(*f*) conducting enhanced ongoing monitoring of the business relationship.

SIMPLIFIED CDD

5.5.1. In general, the full range of CDD measures should be applied to the business relationship. However, if the risk of money laundering or the financing of terrorism is lower (based on the insurance company's own assessment), and if information on the identity of the customer and the beneficial owner is publicly available, or adequate checks and controls exist elsewhere in the Nigerian financial system, it could be reasonable for insurers to apply, subject to these Regulations and the current AML/CFT legislation, simplified or reduced CDD measures when identifying and verifying the identity of the customer, the beneficial owner and other parties to the business relationship.

5.5.2 In lower risk circumstances, insurance companies are required to apply reduced or simplified measures. There is lower risk in circumstances where :

(*a*) The risk of money laundering or terrorist financing is lower ;

(*b*) Information on the identity of the customer and the beneficial owner of a customer is publicly available ;

(*c*) When adequate checks and controls exist elsewhere in national systems.

5.5.3. Examples of Low Risk Customers, Transactions or Products include:

(*a*) Insurance companies provided they are subject to the requirements for combating money laundering and terrorist financing which are consistent with the provisions of these Regulations and are so supervised for compliance ;

(*b*) Public companies (listed on a stock exchange or similar arrangement) that are subject to regulatory disclosure requirements ;

(*c*) Government ministries and parastatals/enterprises ;

(*d*) Life insurance policies where the annual premium is no more than ₦150,000.00 or a single premium of no more than ₦450,000.00 ;

(*e*) Insurance policies for pension schemes if there is no surrender-value clause and policy cannot be used as collateral ;

(*f*) A pension, superannuation or similar scheme that provides retirement benefit to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme ; and

(*g*) Beneficial-owners of pooled-accounts held by Designated Non-Financial Businesses and Professions (DNFBFs) provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the provisions of the Money Laundering (Prohibition) Act 2011.

5.5.4. Insurance companies that apply simplified or reduced CDD measures to customers resident abroad are required to limit such to customers in countries that have effectively implemented FATF Recommendations.

5.5.5. Insurance companies are not permitted to employ Simplified CDD to a customer when there is suspicion of money laundering or terrorist financing or specific higher risk scenarios. In such a circumstance, enhanced due diligence is mandatory.

5.5.6. Insurance companies are to adopt CDD measures on a risk sensitive-basis. They are to determine in each case whether the risks are lower or not, having regard to the type of customer, product, transaction or the

location of the customer. Where there is doubt, insurance companies are directed to clear with NAICOM.

TIMING OF VERIFICATION

5.6.1. Insurance companies are required to verify the identity of the customer, beneficial-owner and occasional customers before or during the course of establishing a business relationship or conducting transaction for them.

5.6.2. Insurance companies are permitted to complete the verification of the identity of the customer and beneficial owner following the establishment of business relationship, only when :

(*a*) This can take place as soon as reasonably practicable ;

(*b*) It is essential not to interrupt the normal business conduct of the customer ; and

(*c*) The money laundering risks can be effectively managed.

5.6.3. Examples of situations where it may be essential not to interrupt the normal conduct of business are :

(*a*) Non face-to-face business ;

(*b*) Life insurance business in relation to identification and verification of the beneficiary under the policy.

5.6.4. Identification and verification of the beneficiary may take place after the insurance contract has been concluded with the policyholder, provided the money laundering risks and financing of terrorism risks are effectively managed. However, in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

5.6.5. Where a policyholder and/or beneficiary is permitted to utilize the business relationship prior to verification, insurance companies are required to adopt risk management procedures concerning the conditions under which this may occur. These procedures should include a set of measures such as a limitation of the number, types and /or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

FAILURE TO COMPLETE CDD

5.7.1. In the event of failure to complete verification of any relevant verification subject or to obtain information on the purpose and intended nature of the business relationship, the insurance company should :

(*a*) not conclude the insurance contract ;

(*b*) not perform the transaction ; or

(*c*) terminate the business relationship and make a suspicious transaction report (STR) to NFIU.

5.7.2. An insurance company that has already commenced the business relationship is required to terminate the business relationship and render suspicious transaction report to NFIU.

ESTABLISHING A BUSINESS RELATIONSHIP

5.8.1. Insurance companies should note that prior to concluding an insurance contract there already exist between the insurer and the policyholder and possibly other parties, a pre-contractual business relationship. Therefore, before a policy is taken out, an insurance company will need to carefully assess the specific background, and other conditions and needs of the customer. To achieve this, the insurer must collect relevant information, for example details of source of funds, income, employment, family situation, medical history, etc. This will lead to a customer profile which could serve as a reference to establish the purpose of the contract and to monitor subsequent transactions and events.

EXISTING CUSTOMERS

5.9.1. Insurance companies are required to apply CDD requirements to existing customers on the basis of materiality and risk and to continue to conduct due diligence on such existing relationships at appropriate times.

5.9.2. The appropriate time to conduct CDD on existing customers is when :

(*a*) transaction of significant values take place :

(*b*) customer documentation standards change substantially ;

(*c*) the insurance company becomes aware that it lacks sufficient information about an existing customer.

5.9.3. Insurance companies are required to properly identify the customer in accordance with these criteria. The customer identification records should be made available to the AML/CFT Chief Compliance Officer or other appropriate staff or competent authorities.

REINSURANCE

5.10. In view of the peculiar nature of reinsurance business which makes it impracticable for the reinsurer to carry out verification of the policyholder or the beneficial owner, reinsurers are allowed to deal with ceding companies that are licensed or otherwise authorized to issue insurance policies, and which have warranted or otherwise confirmed that they apply AML/CFT standards.

ON-GOING DUE DILIGENCE

5.11. The insurance company should perform ongoing due diligence on the business relationship. In general the insurance company should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. It should assess if the change/transaction does not fit the profile of the customer and/or beneficial owner or is for some other reason unusual or suspicious.

MISCELLANEOUS

5.12. Examples of transactions or trigger events after establishment of the contract that require CDD are :

(*i*) a change in beneficiaries (for instance, to include non-family members, or a request for payments to be made to persons other than beneficiaries ;

(*ii*) where there are several overpayments of policy premiums after which the policyholder requests that reimbursement is paid to a third party ;

(*iii*) use of cash and/or payment of large single premiums ;

(*iv*) payment/surrender by a wire transfer from/to foreign parties ;

(*v*) change of address and/or place of residence of the policyholder, in particular, tax residence ;

(*vi*) lump sum top-ups to an existing life insurance contract ;

(*vii*) lump sum contributions to personal pension contracts ;

(*viii*) requests for prepayment of benefits ;

(*ix*) use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution) ;

(*x*) change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment) ;

(*xi*) early surrender of the policy or change of the duration (where this causes penalties or loss of tax relief) ;

(*xii*) request for payment of benefits at the maturity date.

5.12.1. The above list is not exhaustive. Insurance companies should consider other types of transactions or trigger events which are appropriate to their type of business.

5.13. Occurrence of these transactions and events does not imply that (full) customer due diligence needs to be applied. If identification and verification have already been performed, the insurer is entitled to rely on this unless doubts arise about the veracity of that information it holds. For instance, doubts might arise if benefits from one policy of insurance are used to fund the premium payments of another policy of insurance.

5.14. Insurance companies, their directors, officers and employees should not disclose the fact that a suspicious transaction report or related information is being reported, or has been reported, to the NFIU. The insurer should be aware that if it performs additional CDD because of suspicions it could unintentionally tip off the policyholder, beneficiary or other subjects of the suspicious transaction report. The insurance company could then decide not to pursue these due diligence activities but to file a suspicious transaction report.

5.15. Insurance companies should ensure that :

(*a*) there is a clear procedure for staff to report suspicions of money laundering and the financing of terrorism without delay to the Chief Compliance Officer ;

(*b*) there is a clear procedure for reporting suspicions of money laundering and the financing of terrorism without delay to the NFIU; and

(*c*) all staff knows to whom their suspicions should be reported.

5.16. Insurance companies should ensure that the principles applicable to insurance companies also apply to branches and majority owned subsidiaries located outside the country, especially in jurisdictions which do not or insufficiently apply the FATF Recommendations. Thus, branches and majority owned insurance subsidiaries should observe appropriate AML/CFT measures which are consistent with the home jurisdiction requirements. Where local applicable laws and regulations prohibit this implementation, the Commission and NFIU must be informed by the insurance company that it cannot apply the FATF Recommendations.

5.17. Staff should have the level of competence necessary for performing their duties. Insurance companies should ascertain whether they have the appropriate ability and integrity to conduct insurance activities, taking into account potential conflicts of interests and other relevant factors, for instance the financial background of the employee.

5.18. Insurance companies should identify the key staff within their organization with respect to AML/CFT and define fit and proper requirements which these key staff should possess.

5.19. The responsibility for initial and on-going assessment of the fitness and propriety of staff lies with the insurance company. The procedures concerning the assessment of whether staff meets the fit and proper requirements should include the following :

(*a*) verification of the identity of the person involved, and

(*b*) verification of whether the information and references provided by the employee are correct and complete.

5.20. Decisions regarding the employment of key staff should be based on a well founded judgment as to whether they meet the fit and proper requirements.

5.21. Insurance companies should keep records on the identification data obtained about key staff. The records should demonstrate the due diligence performed in relation to the fit and proper requirements.

SUSPICIOUS TRANSACTIONS, COMPLIANCE MONITORING AND RESPONSE TO SUSPICIOUS TRANSACTIONS

Meaning of Suspicious Transaction.

6.1. In these regulations, a *Suspicious Transaction* is one which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering methods. It includes such a transaction that is inconsistent with a policy holder's known legitimate business or personal activities or normal business or that lack obvious economic rationale.

6.1.1. It is extremely difficult to give an exhaustive list of suspicious transactions. An illustrative list of such transactions is however provided in *Appendix IV.*

6.1.2. An important pre-condition of recognition of a suspicious transaction is for the insurance company to know enough about the customer and business relationship to recognize that a transaction, or a series of transactions, is unusual.

6.1.3. Suspicious transactions might fall into one or more of the following examples of categories :

(*a*) any unusual financial activity of the customer in the context of his own usual activities ;

(*b*) any unusual transaction in the course of some usual financial activity ;

(*c*) any unusually linked transactions ;

(*d*) any unusual or disadvantageous early redemption of an insurance policy ;

(*e*) any unusual employment of an intermediary in the course of some usual transaction or financial activity e.g. payment of claims or high commission to an unusual intermediary ;

(*f*) any unusual method of payment ;

(*g*) any involvement of any person subject to international sanctions.

6.1.4. Verification, once begun, should be pursued either to a conclusion or to the point of refusal. If a prospective policyholder does not pursue an application, this may be considered suspicious in itself and must be reported.

Reporting of Suspicious Transactions.

7.1. An Insurance company that suspects or has reasons to suspect : that the funds are the proceeds of a criminal activity, or are related to terrorist financing, is required to report within 7 days its suspicion to the NFIU. All suspicious transactions including attempted transactions are to be reported regardless of the amount involved. The report should include any action taken on the suspicious activity.

7.2. Insurance companies are required to report all transactions in any currency above a threshold of ₦5,000,000.00 Naira or its equivalent for individual and ₦10,000,000.00 Naira or its equivalent for body corporate to NFIU.

7.3. For the purpose of effective industry compliance, where neither suspicious transaction nor currency transaction above the prescribed limit is observed, companies are nevertheless required to file nil report on monthly basis to NFIU.

On-going Training.

8.1. Insurance companies are required to design comprehensive employee education and training programs not only to make employees fully aware of their obligations but also to equip them with relevant skills required for the effective discharge of their AML/CFT compliance tasks.

8.2. Insurance companies should consider what training is appropriate for each individual employee. Some employees may require minimal training on the programme, given their particular details. Others may require a great deal of training. The training should be clearly understood by the employees, agents, brokers, and others doing business with the company. The CCO should be available to answer all questions pose by employees. It is important to state that the training should be on going so as to keep pace with the dynamism of money laundering and terrorism financing.

8.3. The employee training programs are required to be developed under the guidance of the AML/CFT Chief Compliance Officer in collaboration with the top Management. The basic elements of the employee training program are expected to include :

(*a*) AML/CFT legislation ;

(*b*) The nature of money laundering ;

(*c*) Money laundering 'red flags' and suspicious transactions ;

(*d*) Trade-based money laundering typologies ;

(*e*) Reporting requirements ;

(*f*) Policy holder due diligence / Enhanced Customer Due Diligence (EDD) on high risk persons and products ;

(*g*) Risk-based approach to AML/CFT ;

(*h*) Record keeping and retention policy ;

(*i*) General understanding of the insurance company's AML/CFT policy and procedures with particular emphasis on verification and recognition of suspicious customer transactions and the need to report suspicions to the Chief Compliance Officer.

8.4. Employees who on account of their assigned work, require more specific training can be divided into two categories. The first category are those staff involved in underwriting, premiums collection and payment of claims. The second category involves directors and senior management staff with responsibilities for management supervision and system auditing.

8.5. The staff category mentioned in 8.4 above need to be aware of their legal responsibilities in relation AML/CFT generally, and should be conversant with the company's AML/CFT policies and procedures. In particular , they need to understand the client acceptance policies and procedures, the requirements of verification and record keeping, the recognition and reporting of suspicious customers/transactions and suspicion of the financing of terrorism. They also need to know that suspicions should be reported to the Chief Compliance Officer in accordance with the insurance company's AML/CFT policies and procedures.

8.6. A higher level of instruction covering all aspects of AML/CFT policy and procedure should be provided to the staff in the second category. The required training should therefore include knowledge of :

(*a*) their responsibility regarding AML/CFT policies and procedures ;
(*b*) relevant laws, including the offences and penalties ;
(*c*) procedures relating to the service of production and restraint orders ;
(*d*) internal reporting procedures, and
(*e*) the requirements for verification and record keeping.

8.7. In addition to the training mentioned in the previous paragraphs, the Chief Compliance Officer should receive in-depth training concerning all relevant legislation and guidance, and AML/CFT policies and procedures. The Chief Compliance Officer will require extensive initial and continuing instruction on the validation and reporting of suspicious customers/transactions and freezing assets in accordance with current AML/CFT legislations.

8.8. To ensure maximum compliance with the training requirements of current AML/CFT legislations, all staff of Insurance Broking firms must receive AML/CFT training on on-going basis. Evidence of staff attendance to a minimum of two NAICOM approved trainings in each year shall be a condition for renewal of annual license.

8.9. Insurance Companies are required to submit their Annual AML/CFT Employee training program to the NAICOM and NFIU not later than the 31st of December every financial year against the next year.

Record Keeping.

9.1. Insurance companies are required to maintain all necessary records of transactions, both domestic and international, for at least five (5) years following completion of the transaction (or longer if requested by the NAICOM and NFIU in specific cases). This requirement applies regardless of whether the contract or business relationship is ongoing or has been terminated.

9.2. The records of transaction required to be maintained by insurance companies will include the risk profile of each customer and/or beneficial owner and the data obtained through the CDD process (e.g. name, address, the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction), official identification documents (such as passports, identity cards or similar documents), and business correspondence.

9.3. Insurance companies should implement specific procedures for retaining internal records of transactions both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity. In the case of long term insurance, full documentary evidence is usually retained based on material completed at the initiation of the proposal of the contract, together with evidence of processing of the contract up to the point of maturity.

9.4. Insurers shall retain the records of those contracts, which have been settled by claim (maturity or death), surrender or cancellation, for a period of at least 10 years after that settlement.

9.5. In situation where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed where practicable.

9.6. In case of policy holder identification data obtained through the policy holder due diligence process, account files and business correspondence should be retained for at least 10 years after the business relationship is ended.

9.7. Insurance companies should ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of clients or business relationships.

9.8. Insurance companies should ensure that they have adequate procedures :

(*a*) to access initial proposal documentation including, where these are completed, the client financial assessment, client needs analysis, copies of regulatory documentation, details of the payment method, illustration of benefits, and copies of documentation in support of verification by the insurance companies.

(*b*) to access all post-sale records associated with the maintenance of the contract, up to and including maturity of the contract, and

(*c*) to access details of the maturity processing and/or claim settlement including completed "discharge documentation".

Chief Compliance Officer's Designation and Duties.

10.1. Each Insurance company is required to designate its AML/CFT Chief Compliance Officer with the *relevant competence, authority and independence* to implement the company's AML/CFT compliance Program.

10.2. To ensure a measure of authority and independence for the function, the Chief Compliance Officer must not be below the status of Assistance General Manager (AGM).

10.3. The duties of the AML/CFT Chief Compliance Officer, among others, include :

(*i*) Developing an AML/CFT Compliance Program ;

(*ii*) Receiving and vetting suspicious transaction reports from staff ;

(*iii*) Filing suspicious transaction reports with the NFIU ;

(*iv*) Rendering "nil" reports with the NFIU, where necessary to ensure compliance ;

(*v*) Ensuring that the insurance company's compliance program is implemented ;

(*vi*) Co-co-ordinating the training of staff in AML/CFT awareness, detection methods and reporting requirements ; and

(*vii*) Serving both as a liaison officer for NAICOM and NFIU and a point-of contact for all employees on issues relating to money laundering and terrorist financing.

Internal Control / Audit

11.1. Insurance companies are required to carry out on a regular basis, independent review of their AML/CFT program. This can be performed by its internal audit/inspection departments or qualified and experience consultant. The report should specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects. Exception reporting under AML policy should be made to Audit Committee of the Board.

Relationship with Agents and Brokers.

12.1. The obligation to identify and report suspicious transaction applies only to an insurance company and not to its agents or brokers. Nevertheless, given that insurance agents and brokers are an integral part of the insurance industry due to their direct contact with customers, insurance companies are required to structure and implement their policies and procedure in such a way as to obtain customer related information necessary to detect suspicious transactions from all relevant sources, including from its agents and brokers, and to report suspicious transactions based on such information.

12.2. Insurance companies may rely on intermediaries and third parties to perform the following CDD elements :

(*a*) identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information ;

(*b*) identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner to the extent the intermediary or third party is satisfied ;

(*c*) know who the beneficial owner is, including taking reasonable measures to understand ;

(*d*) the ownership and control structure of the customer, and

(*e*) obtaining information on the purpose and intended nature of the business relationship

12.3. When reliance on intermediaries and third parties is used the insurance companies should immediately :

(*a*) obtain the necessary information concerning the above mentioned elements.

(*b*) take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the intermediaries and third parties upon request without delay.

(*c*) be satisfied with the quality of the due diligence undertaken by the intermediaries and third parties.

(*d*) satisfy itself that the intermediaries and third parties are regulated and supervised, and have measures in place to comply with CDD requirements.

12.4. Where such reliance is used, the ultimate responsibility for customer and/or beneficial owner identification and verification remains with the insurance company relying on the intermediaries or third parties. The checks by the insurance company as indicated in the previous paragraph do not have to consist of a check of every individual transaction by the intermediary or third party. The insurance company only needs to be satisfied that the AML and CFT measures are implemented and operating adequately.

12.5. Insurance companies should satisfy the above provisions by including specific clauses in the agreements with intermediaries/third parties or by any other appropriate means. These clauses should include commitments for the intermediaries/third parties to perform the necessary CDD measures, granting access to client files and sending (copies of) files to the insurer upon request without delay. The agreement could also include other compliance issues such as reporting to the insurance company observed suspicious transactions.

12.6. NAICOM will determine which intermediaries and third that can perform the required CDD. However, the insurance company should undertake and complete its own verification of the customer and beneficial owner if it has any doubts about the ability of the intermediary or the third party to undertake appropriate due diligence.

12.7. To this end, insurance companies are required to have in place comprehensive Manuals on the procedures for selling insurance products, policy holder identification, record-keeping, acceptance and processing of insurance proposals, issuance of insurance policies amongst other things. When faced with a non-compliant agent or broker. an insurance company is required to take necessary actions to secure such compliance, including, when appropriate, terminating its business relationship with such an agent or broker and reporting same to NAICOM and NFIU.

New Technology and Non Face-to-face Transactions.

13.1. Insurance companies are required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes such as internationally accepted Credit or Debit Cards and Mobile Telephone Banking systems for the purpose of money laundering and terrorist financing.

13.2. Insurance companies are required to have policies and procedures in place to address any specific risks associated with non-face-face business relationship or transactions. These policies and procedures shall be applied automatically when establishing policy holder relationships and conducting

ongoing due diligence. Measures for managing the risks should include specific and effective CDD procedures that apply to non-face-face policy holders.

Offshore Operations.

14.1. In relation to offshore operations, Insurance companies are required to, in addition to performing the normal KYP requirements, take the following measures :

(*a*) Gather sufficient information about the offshore institution to understand fully the nature of its business; and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether or not it has been subject to a money laundering or terrorist financing investigation or regulatory action.

(*b*) Assess the offshore institution's AML/CFT- controls and ascertain that the latter are in compliance with FATF standards.

(*c*) Ensure the local institution obtained approval from NAICOM before establishing offshore or entering into any agreement with a foreign insurance company.

(*d*) Document the respective AML/CFT responsibilities of such institution.

Politically Exposed Persons (PEPS).

15.1. PEPS are individuals who are or have been entrusted with prominent public functions both in Nigeria and foreign countries and those associated with them. Examples of PEPs include, but are not limited to :

(*a*) Heads of State of Government ;

(*b*) Governors ;

(*c*) Local Government Chairmen ;

(*d*) Senior Politicians ;

(*e*) Senior Government Officials ;

(*f*) Judicial or Military or Para-military officials from the rank of a major or equivalent ;

(*g*) Senior Executives of State owned Corporations ;

(*h*) Important political party officials ;

(*i*) Family members or close associates of PEPs ; and

(*j*) Members of Royal Families.

15.2. Insurance Companies are required, in addition to performing CDD measures, to put in place appropriate risk management systems to determine whether a potential policy holder or existing policy holder or the beneficial owner is a politically exposed person. The board of directors of the insurer must establish a client acceptance policy with regard to PEPs, taking account of the reputational and other relevant risks involved.

15.3. Insurance Companies are also required to obtain senior management approval before they establish business relationships with PEPs and to render quarterly returns on their transactions with PEPs to NAICOM and NFIU.

15.4. Where a policy holder has been accepted or has an ongoing relationship with the insurance company and the policy holder or beneficial owner is subsequently found to be or becomes PEP ; the insurance company is required to obtain senior management approval in order to continue the business relationship.

15.5. Insurance Companies are required to take reasonable measures to establish the source of wealth and the sources of funds of policy holders and beneficial-owners identified as PEPs and report all anomalies immediately to the NAICOM and other relevant authorities.

15.6. An Insurance Company in a business relationship with PEP is required to conduct enhanced on-going monitoring of that relationship. In the event of any transaction that is abnormal, Insurance Companies are required to flag the contract and to report immediately to NAICOM and NFIU.

Risk Classification of Policyholders.

16.1. In the context of the very large base of insurance policy holders and the significant differences in the extent of risk posed by them, the insurance companies are advised to classify the policy holders into high, medium and low risk, based on the individual's profile and product profile, to decide upon the extent of due diligence.

16.2. The insurance's company's strategic policies will determine its exposure to risks such as underwriting risk, reputational risk, operational risk, concentration risk and legal risk. After determining the strategic policies, client acceptance policies should be established, taking account of risk factors such as the background and geographical base of the customer and/or beneficial owner and the complexity of the business relationship. AML/CFT control measures and procedures should therefore be an integral part of the overall customer due diligence and enterprise risk management of the insurance company.

16.3. The extent and specific form of these measures may be determined following a risk analysis based upon relevant factors including the customer, the business relationship and the transaction(s). Enhanced due diligence is called for with respect to higher risk categories. Decisions taken on establishing relationships with higher risk customers and/or beneficial.owners should be taken by senior management. Depending on the circumstances the insurance company may apply reduced or simplified measures in the case of low risk categories.

16.4. Prior to the establishment of a business relationship, the insurer should assess the characteristics of the required product, the purpose and nature of the business relationship and any other relevant factors in order to create and maintain a risk profile of the customer relationship. Based on this assessment, the insurer should decide whether or not to accept the business relationship. As a matter of principle, insurers should not offer insurance to customers or beneficiaries that obviously use fictitious names or whose identity is kept anonymous.

16.5. There are some factors that must be considered by insurance companies when creating a risk profile, and these are not in any order of importance and the factors listed in these Regulations are not exhaustive and include where appropriate the following :

(*a*) Type and background of customer and/or beneficial owner.

(*b*) The customer's and/or beneficial owner's geographical base.

(*c*) The geographical sphere of the activities of the customer and/or beneficial owner.

(*d*) The nature of the activities .

(*e*) The means of payment as well as the type of payment (cash, wire transfer, cheque or other means of payment).

(*f*) The source of funds.

(*g*) The source of wealth.

(*h*) The frequency and scale of activity.

(*i*) The type and complexity of the business relationship.

(*j*) Whether or not payments will be made to third parties.

(*k*) Whether a business relationship is dormant.

(*l*) Any bearer arrangements.

(*m*) Suspicion or knowledge of money laundering, financing of terrorism or other crime.

16.6. When the identity of customers and beneficial owners with respect to the insurance contract has been established the insurance company is able to assess the risk to its business by checking customers and beneficial owners against internal and external information on known fraudsters or money launderers and on known or suspected terrorists (publicly available on sanctions lists such as those published by the United Nations).

16.7. Insurance companies must use available sources of information when considering whether or not to accept a risk. Identification and subsequent verification will also prevent anonymity of policyholders or beneficiaries and the use of fictitious names.

(*i*) For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose contracts by and large conform to the known profile may be categorized as low risk. Illustrative examples of low risk policy holders could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society, Government departments and Government owned companies, regulators and statutory bodies, etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the policy holder are to be met. Notwithstanding the above, in case of continuing policies, if the situation warrants, as for example if the policy holder profile is inconsistent with his investment through top-ups, a re-look on policy holder profile is to be carried out.

(*ii*) For the high risk profiles, like for policy holders who are non-residents, high net worth individuals, trusts, charities, NGO's and Organizations receiving donations, companies having close family shareholding or beneficial ownership, firms with sleeping partners, politically exposed persons (PEPs), and those with dubious reputation as per available public information who need higher due diligence, KYC and underwriting procedures should ensure higher verification and counter checks. In this connection insurers are also advised to carry out the appropriate level of due diligence keeping the observations at 15.5 in view.

Covered Products.

17.1. The AML/CFT requirements focus on the vulnerability of the products offered by the insurers to any of the processes of money laundering or terrorism financing. Some vulnerable products are illustrated in *Appendix II*. Based on the vulnerability criterion, the following categories of products, for the time being are not covered under the AML/CFT requirements :

(*i*) Stand alone medical/health insurance products.

(*ii*) Re-insurance and retrocession contracts where the treaties are between insurance companies for reallocation of risks within the insurance industry and do not involve transactions with policy holders.

(*iii*) Group insurance businesses which are typically issued to a company, financial institution, or association and generally restrict the ability of an individual insured or participant to manipulate their investment.

(*iv*) Term life insurance contracts, in view of the absence of currency surrender value and stricter underwriting norms for term policies (especially those with large amounts).

Sources of Funds.

18.1. It is imperative to ensure that the insurance being purchased is reasonable. Accordingly, policy holder's source of funds, his estimated net worth, etc., should be documented properly and the advisor and/or employee

shall obtain income proofs as in *Appendix III*, to establish his need for insurance cover. Proposal form may also have questionnaires /declarations on sources of fund, and details of bank accounts. Large single premiums should be backed by documentation, to establish source of funds.

Proposal Form should, at minimum, contain the following information :

(*a*) Name of the insured ;

(*b*) Full address ;

(*c*) Product/service sought ;

(*d*) Source of funds ;

(*e*) Expected premium ;

(*f*) Bankers ;

(*g*) Means of identification ;

(*h*) Client's risk category.

Attention on Complex and Unusual Large Transactions.

19.1. Insurance companies are required to pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. Examples of such transactions or patterns of transactions include significant transactions that exceed certain limits.

19.2. Insurance companies are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. They are required to report such findings to NAICOM and NFIU; and keep them available for NAICOM, NFIU, other competent authorities and auditors for at least five years.

19.3. All insurance companies effecting transfers/payments/remittance to foreign insurance companies, re-insurance companies, etc must obtain letter of attestation from NAICOM before consummating such transaction(s).

Verification at the Time of Redemption/ Surrender.

20.1. In life insurance business, no payments should be allowed to 3rd parties except in cases like superannuation/gratuity accumulations and payments to legal heirs in case of death benefits. All payments, should be made after due verification of the bona fide beneficiary, through account payee cheques.

(ii) Policy cancellations need particular attention of insurer especially in client/agents indulging in policy surrender on more than one occasion.

(iii) AML checks become more important in case the policy has been assigned by the policyholder to a third party not related to him (except where the assignment is to Banks/FIs/Capital Market intermediaries).

SANCTIONS

21.1. Pursuant to the provisions of the National Insurance Commission Act 1997 and Insurance Act 2003, contravention of any of the provisions of these regulations shall attract in respect of insurance companies, a fine in the sum of ₦500, 000. This is in addition to any other specific punishment under the provision of the current AML/ CFT legislations. Against Insurance Companies.

21.2. Any person being a director, senior management, manager or other employee of an insurance company, who, either acting alone or in partnership with others, contravenes the provisions of these regulations under any circumstances, shall be subject to any or all of the following sanctions : Against the Officers.

(*a*) On the first infraction, *be warned in writing by the* NAICOM.

(*b*) On the second infraction, his/her appointment will be directed by NAICOM to be terminated and he/she be blacklisted from working in the insurance industry ; and

(*c*) In each instance, the names of the officers penalized shall be reflected in the company's financial statements and published in the newspapers.

(*d*) The officer shall also be reported to the professional body he or she belongs to, for appropriate disciplinary action.

21.3. In addition to the above regulatory sanctions by NAICOM, particulars of the insurance company and/or individual(s) involved shall be forwarded to the relevant authorities such as EFCC, NPF, ICPC, etc for possible criminal investigation and prosecution.

DEFINITIONS

22.1. Money laundering is the processing of criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source. Terrorist Financing (TF) includes the financing of terrorist acts, and of terrorists and terrorist organizations. AML/CFT Defined.

22.2. "*An applicant for Business*" means the person or company seeking to establish a 'business relationship' or an occasional policy holder undertaking a 'one-off' transaction whose identity must be verified. Applicant for Business

22.3. "*Business Relationship*" means any arrangement between the insurance company and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a 'frequent, habitual or regular' basis, and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset. Business Relationship.

Covered Products.

22.4. The term "*Covered Product*" means :

(*a*) A permanent Life Insurance policy, other than a group Life Insurance Policy ;

(*b*) An annuity Contract, other than a Group Annuity Contract ; and

(*c*) Any other insurance products with cash value or investment features.

22.5. "*Insurance Company*" or "*Insurer*" means a company that engages in the business of issuing or underwriting of insurance products and is registered by NAICOM.

22.6. "*Insurer*" also includes "*Reinsurer*".

One-off Transactions.

22.7. The term "*Not Covered Products*" includes :

(*a*) Group Life Insurance products.

(b) Charitable annuities.

(*c*) Term Life Assurance.

(*d*) Property, personal accident, health or titled insurance.

(*e*) Re-insurance and retrocession contracts between companies not involving policy holders.

22.8. A 'one-off transaction' means any transaction carried out other than in the course of an established business relationship.

22.9 "*Client*" also means "*Policyholder*"

22.10. "*Current* AML/CFT *legislations*" means :

(*a*) The Money Laundering (Prohibition) Act 2011, and

(*b*) Terrorism (Prevention) Act 2011.

ABBREVIATIONS

AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
CDD	Policyholder Due Diligence
CTR	Currency Transaction Report
EFCC	Economic and Financial Crimes Commission
FATF	Financial Action Task Force
NFIU	Nigerian Financial Intelligence Unit
FT	Financing of Terrorism
KYPG	Know Your Policyholder Guideline
ML	Money Laundering
MLPA	Money Laundering (Prohibition) Act, 2004
NCCT	Non-Co-operative Countries and Territories
NDLEA	National Drug Law Enforcement Agency

NIA	National Intelligence Agency
NAICOM	National Insurance Commission
PEP	Politically Exposed Person
DSS	Department of States Service
STR	Suspicious Transactions Report
G-AML/CFT	Guidance notes on Anti-Money Laundering and Combating the Financing of Terrorism
IAIS	International Association of Insurance Supervisors.

Policy Holder Identification Procedure

Documents that may be obtained from Policy Holders

Features	*Documents*
Insurance Contracts with individuals • Name!	(*i*) Passport. (*ii*) National Identity Card. (*iii*) Voter Registration Card. (*iv*) Driving License. (*v*) Letter from a recognized public authority or public servant verifying the identity and residence of the policy holder.
• Proof of Residence	(*i*) Telephone bill. (*ii*) Bank account statement. (*iii*) Letter from any recognized public authority (*iv*) Electricity bill. (*v*) Tenancy Agreement.
Insurance Contracts with companies Name of the company • Principal place of business • Mailing address of the company • Telephone/Fax Number	(*i*) Certificate of incorporation and Memorandum and Articles of Association. (*ii*) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account. (*iii*) Power of Attorney granted to its managers, officers or employees to transact business on its behalf.
Insurance Contracts with partnership firms • Name • Address • Names of all partners and their addresses • Telephone numbers of the firm and partners	(*i*) Registration certificate, if registered. (*ii*) Partnership Deed. (*iii*) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf. (*iv*) Any officially valid document identifying the partners and the personsholding the Power of Attorney and their Addresses

Insurance Contracts with trusts and foundations. Names of trustees, beneficiaries and signatories. Names and addresses of the founder, the Managers/Directors and the beneficiaries Telephone/ fax numbers.	(*i*) Certificate of registration, if registered (*ii*) Power of Attorney granted to transact business on its behalf. (*iii*) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/ Managers/Directors and their addresses. (*iv*) Resolution of the managing body of the foundation/association.

Appendix II

EXAMPLES OF VULNERABLE PRODUCTS

1. Unit linked products which provide for withdrawals and unlimited top up premiums ;

2. Single premium products, where the money is invested in lump sum and surrendered at the earliest opportunity.

Appendix III

Income Proofs

Standard Income Proofs :

Income tax assessment orders/Income Tax Returns
Employer's Certificate
Audited Company accounts
Audited firm accounts and Partnership Deed

Non-standard Income Proofs :

Chartered Accountant's Certificate
Agricultural Income Certificate
Agricultural-land details and Income assessments
Bank Currency-flows statements, Pass-book
Debenture Certificate
Dividend Warrant
Bond Certificate
Share Certificate

Appendix IV

ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS

1. Policy holder insisting on anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information.
2. Currency based suspicious transactions for payment of premium and top ups over and above ₦500, 000 per person per policy ;
3. Frequent policy surrenders by policyholders ;
4. Assignments to unrelated parties without valid consideration ;
5. Request for a purchase of policy in amount considered beyond his apparent need ;
6. Policy from a place where he does not reside or is employed ;
7. Unusual terminating of policies and refunds ;
8. Frequent request for change in addresses ;
9. Borrowing the maximum amount against a policy soon after buying it;
10. Inflated or totally fraudulent claims e.g. by arson or other means : Causing a fraudulent claim to be made to recover part of the Invested illegitimate funds ;
11. Overpayment of premiums with a request for a refund of the amount overpaid.

MADE at Abuja this 30th day of January, 2012.

FOLA DANIEL
Commissioner for Insurance

PART B

KNOW YOUR POLICY HOLDER GUIDANCE NOTES

ARRANGEMENT OF SECTIONS

KNOW YOUR POLICYHOLDER (KYP) GUIDANCE NOTES FOR INSURANCE INDUSTRY IN NIGERIA

1.0. Introduction

1.0.1. This manual is intended to serve as a further guide to insurance companies in Nigeria on the procedures necessary for the proper knowledge of their policy holders. Having sufficient information about your policy holder and making use of that information is the most effective weapon against being used to launder the proceeds of crime. In addition to minimizing the risks of being used for illicit activities, it provides protection against fraud, reputational and financial risks and enables individual insurance companies to recognize and deal with activities that are out of tune. This document has also stated the procedure for conducting policy holder due diligence.

1.0.2. Insurance companies should not establish a business relationship until all relevant parties to the relationship have been identified and the nature of the businesses they intend to conduct have been ascertained. Once an ongoing business relationship has been established, any activity that is inconsistent with the norm must be further examined to eliminate suspicion of money laundering.

1.0.3. Insurance companies should ensure that their proposal form contain a list of KYP documentary requirements, which their clients are to provide at the point of commencing relationship.

The Duty to Obtain Identification Evidence.

1.1.1. The first requirement of knowing your policy holder for AML/CFT purposes is for the insurance company to be satisfied that a prospective policy holder is who he/she claims to be.

1.1.2. Insurance companies should not carry out, or agree to carry out, insurance business or provide advice to a policy holder or potential policy holder, unless they are certain as to who that person actually is. If the policy holder is acting on behalf of another, e.g. someone else is paying policy premium, or the policy is to be held in the name of someone else, then the insurance company has the obligation to verify the identity of both the policy holder and the intermediaries unless the policy holder is itself a Nigerian regulated insurance company.

1.1.3. Although insurance companies have the duty to obtain evidence in respect of their policy holders, there are certain exceptions to this duty as set out in Section 9 of this Manual. However, since exemptions are difficult to apply, insurance companies are advised to identify all relevant parties to the relationship from the outset. The general principles and means of obtaining satisfactory identification evidence are also set out below.

The Nature and level of the business to be conducted.

1.2.1. Sufficient information should be obtained on the nature of the business that the policy holder intends to undertake, including the expected or predictable pattern of transactions.

1.2.2. The information collected at the outset for this purpose should include:

(*a*) Purpose and reason for the policy establishing the relationship;

(*b*) Nature and type of the insurance business that is to be undertaken;

(*c*) Expected origin of the funds to be used to pay the premium during the relationship; and

(*d*) Details of occupation/employment/business activities and sources of wealth or income.

1.2.3. Reasonable steps should be taken to keep the information up to date as the opportunities arise, e.g. when an existing policy holder takes up additional/new insurance product/policy. Such information obtained during any meeting, discussion or other communication with the policy holder should be recorded and kept in the policy holder's file to ensure, as far as practicable, that current policy holder information is readily accessible to the NAICOM Relationship /Compliance Officer (NRO) or relevant regulatory bodies.

Application of Commercial Judgment.

1.3.1. Insurance companies are advised to take a risk-based approach to the 'Know Your Policy Holders' requirements. Decisions should be taken on the number of times to verify the subjects within a relationship, the identification evidence required, and when additional checks are necessary. For example, for group policy relationships, all joint policyholders need to be verified; where practicable for a company or partnership, all focus should be on the principal owners /controllers whose identities need to be verified.

1.3.2. The identification evidence collected at the outset should be viewed against the inherent risks in the business or service.

2.0. Establishing Identity

Identification Evidence.

2.1.1. It is important to note that the policy holder identification process should not start and end at the point of application but should continue as far as the business relationship subsists. The process of confirming and updating identity and address, and the extent of additional KYP information collected will however differ from one type of insurance company to another.

2.1.2. The general principles for establishing the identity of both legal and natural persons, and the guidance on obtaining satisfactory identification evidence set out in this manual are by no means exhaustive.

What is Identity.

2.2.1. Identity generally means a set of attributes such as names used, date of birth/incorporated and the residential/business address where the policy

holder can be located. These are features, which can uniquely identify a natural or legal person.

2.2.2. In the case of a natural person, the date of birth should be obtained as an important identifier in support of the name. There is however no compulsion to verify the date of birth provided by the policy holder.

2.2.3. Where an international passport/national identity card is taken as evidence of identity, the number, date and place/country of issue (as well as expiring date in the case of international passport) should be recorded.

When must Identity be Verified.

2.3.1. Identity must be verified whenever a business relationship is to be established, or a one-off transaction or series of linked transactions are undertaken. It should be noted that transaction in this manual is defined to include the giving of advice. However, advice is not intended to apply to the provision of information about the availability of products or services or to apply to a first interview/discussion prior to establishing a relationship.

2.3.2. Once identification procedures have been satisfactorily completed, and the business relationship established, as long as contact or activity is maintained and records concerning that policy holder are kept, no further evidence of identity is needed when transaction or activity is subsequently undertaken.

Redemptions/ Surrenders.

2.4.1. When a policy holder finally realizes his investment, surrenders his life policy or policy attains maturity or to be paid claims (wholly or partially), if the amount payable is in excess of ₦5 million for an individual and ₦10 million for a body corporate, or such other monetary amounts as may from time to time be stipulated by applicable money laundering legislation, the identity of the policy holder must be verified and recorded if it had not been done previously.

In the case of redemption of an investment or surrender of policy (wholly or partially), the insurance company will be considered to have taken reasonable measures to establish the identity of the policy holder/investor where payment is made to the legal owner of the claims/surrender/policy proceeds by means of a cheque crossed" account payee".

Whose Identity should be Verified.

2.5.1. (*a*) *Policy holders*—Sufficient evidence of the identity must be obtained to ascertain that the client is who he/she claims to be.

(*b*) *The intermediary acting on behalf of another*—The obligation is to obtain sufficient evidence of (both) their identities. This rule is however, subject to some exceptions e.g. in co-insurance where the lead underwriter/ broker supplied the normal placement slip.

2.5.2. There is no obligation to look beyond the policy holder where :

(*a*) It is acting on its own account (rather than for a specific client or group of clients) ;

(*b*) The client is an Insurance Company; Reinsurance Company or other regulated insurance companies ; and

(*c*) All the business is to be undertaken in the name of a regulated insurance company.

2.5.3. In other circumstances, unless the client is a regulated insurance company acting as broker or intermediary on behalf of one or more underlying clients within Nigeria, and has given written assurance that it has obtained and recorded evidence of identity to the required standards, identification evidence should be verified for :

(*a*) The named policy holder/insured in whose name the policy is issued ;

(*b*) Any principal beneficial owner of policy being insured who is not the policy holder or named insured ;

(*c*) The principal controller(s) of business relationship (*i.e.* those who regularly provide instructions) ; and

(*d*) Any intermediate parties (*e.g.* where the fund is managed or owned by an intermediary).

(*e*) Appropriate steps should also be taken to identify directors.

2.5.4. Joint Applicants/Policy Holders—Identification evidence should be obtained for all the policy holders.

2.5.5. Higher risk business undertaken for private companies (*i.e.* those not listed on the stock exchange)—sufficient evidence of identity and address should be verified in respect of :

(*a*) The principal underlying beneficial owner(s) of the company-5 *per cent* interest and above ; and

(*b*) Those with principal control over the company's assets (*e.g.* principal controllers/directors).

(*c*) Insurance companies should be alert to circumstances that might indicate any significant changes in the nature of the business or its ownership and make enquiries accordingly.

Deposit Administrations (DA).

2.5.6. Insurance companies should obtain and verify the identity of those providing funds for deposit administration and those who are authorized to invest or transfer the funds, or make decisions on behalf of the insured, the principal (DA managers) who have power to redeem or roll over the deposit.

2.5.7. Regular life policy-life policy in the name of third parties.

2.5.8. When the policyholder takes an insurance, a regular life policy scheme whereby the premium are paid by one person for a policy in the name of another (such as a spouse or a child), the person who pays the premium or makes deposit into the scheme should be regarded as the applicant for business for whom identification evidence must be obtained in addition to the legal owner.

Personal Pension Schemes.

2.6.1. Identification evidence must be obtained at the outset for all life policies and personal pensions connected to a policy of insurance and taken out by virtue of a contract of employment of pension scheme.

2.6.2. Personal pension advisers are also charged with the responsibility of obtaining the identification evidence on behalf of the pension fund provider. Confirmation that identification evidence has been taken should be given on the transfer of a pension to another provider.

Timing of Identification Requirements.

2.7.1. An acceptable time span for obtaining satisfactory evidence of identity will be determined by the nature of the business, the geographical location of the parties and whether it is possible to obtain the evidence before commitments are made or money changes hands. However, any occasion when business is conducted before satisfactory evidence of identity has been obtained must be exceptional and can only be those circumstances justified with regard to the risk.

To this end, insurance companies must :

(*i*) Obtain identification evidence as soon as reasonably practicable after it has contact with a client with a view to :

(*a*) Agreeing with the client to carry out an initial transaction ; or

(*b*) Reaching an understanding (whether binding or not) with the client that it may carry out future transactions ;

(*ii*) Where the client does not supply the required information as stipulated in (*i*) above the insurance company, must :

(*a*) Discontinue any activity it is conducting for the client ; and

(*b*) Bring to an end any understanding reached with the client.

2.7.2. An insurance company may however start processing the business or application immediately, provided that it :

(*i*) Promptly takes appropriate steps to obtain identification evidence ; and

(*ii*) Does not transfer or pay any money out to a third party until the identification requirements have been satisfied.

2.7.3. The failure or refusal by an applicant to provide satisfactory identification or evidence within a reasonable time frame and without adequate explanation may lead to a suspicion that the policy holder or insured is engaged in money laundering. The insurance company should therefore make a suspicious activity report to the NAICOM, NFIU and NDLEA based on the information in their possession before any funds are returned to where they came from.

2.7.4. Insurance companies should adopt consistent policies of closing a relationship or unwinding a transaction where satisfactory evidence of identity cannot be obtained.

2.7.5. Insurance companies are enjoined to respond promptly to enquiries relating to the identity of their policy holders.

Cancellation/ Cooling Off Period.

2.8.1. Where a policyholder exercises surrender/cancellation of policy rights or cooling off period, the sum for the premium must be repaid (subject to some deductions where applicable). Since cancellation /cooling off period could offer a readily available route for laundering money, insurance companies should be alert to any abnormal exercise of these rights by a policyholder, or in respect of business introduced through an intermediary. In the event that abnormal exercise of these rights become(s) apparent, the matter should be treated as suspicious and reported to the appropriate authorities.

3.0. Identification Procedures

General Principles.

3.1.1. An insurance company should ensure that it is dealing with a real person(s) or organization (natural, corporate or legal), by obtaining sufficient identification evidence. When reliance is being placed on third party to identify or confirm the identity of a client, the overall legal responsibility for obtaining satisfactory identification evidence rests with the insurance company.

3.1.2. The requirement in all cases is to obtain satisfactory evidence that a person of that name lives at the address given and that the applicant is that person, or that the company has identifiable owners and that its representatives can be located at the address provided.

3.1.3. Because no single form of identification can be fully guaranteed as genuine, representing correct identity, the identification process should be cumulative.

3.1.4. The procedures adopted to verify the identity of private individuals should state whether identification was done face to face or remotely. Reasonable steps should be taken to avoid single or multiple fictitious policy or substitution (impersonation) fraud.

3.1.5. An introduction from a respected policy holder, personally known to a Director or Manager, or from a member of staff, will often provide comfort but must not replace the need for identification evidence set out in Section 4 of this guidance note. Details of who initiated and authorized the introduction should be kept in the policy holder's Mandate File along with other records. Directors/Senior Managers must insist on normal identification procedures for every applicant.

3.2. New Policy for Existing Policy Holders

3.2.1. When an existing policyholder surrenders or cancels a policy and/or takes up another, or enters into a new agreement to take-up another policy products or services, there is no need to verify the identity or address for such a policy holder unless the name or the address provided does not tally with the information in the insurance company's records. However, procedures should be put in place to guard against impersonation fraud and the opportunity of the new polices should also be taken to ask the policy holder to confirm the relevant details and obtain any missing KYP information. This is particularly important :

(*i*) If there was an existing business relationship with the policyholder and identification evidence had not previously been obtained ; or

(*ii*) If there had been no recent contact or correspondence with the policyholder, e.g. within the past six months ; or

(*iii*) When a previously lapsed policy is re-activated.

3.2.2. In the circumstances above, details of the previous policy(s) and any identification evidence previously obtained, or any introduction records, should be linked to the new policy records and retained for the prescribed period in accordance with the provision of Insurance Policy Guidelines.

3.3. Certification of Identification Documents

3.3.1. To guard against the dangers of postal intercept and fraud, prospective policyholder should not be asked to send by post originals of valuable personal identity documents (e.g. International Passport, Identity Card, Driving Licence, etc).

3.3.2. Where there is no fact-to-face contact, with the client, and documentary evidence is required, copies certified by a lawyer, notary public/ court of competent jurisdiction, banker, accountant, senior public servant, senior insurance practitioner or their equivalent in the private sector, should be obtained. The person undertaking the certification must be known and capable of being contacted if necessary.

3.3.3. In the case of foreign nationals, the copy of international passport, national identity card or documentary evidence of address should be certified by :

(*i*) An embassy, consulate or high commission of the country of issue ; or

(*ii*) A senior official within the insurance company ; or

(*iii*) A lawyer, attorney or notary public.

3.3.4. Certified copies of identification evidence should be stamped, dated and signed, "Original sighted by me", by a senior officer of the insurance company. Insurance companies should always ensure that a good reproduction of photographic evidence of identity is obtained and where this is not possible, a copy of the evidence certified as proving a good likeness of the applicant.

3.4. Records of Identification Evidence

3.4.1. Records of the supporting evidence and methods used to verify identity must be retained for ten years after the maturity of the policy or payment of claims or the end of the business relationship.

3.4.2. Where the supporting evidence could not be copied at the time it was obtained, the reference numbers and other relevant details of the identification evidence obtained should be recorded to enable the documents to be re-obtained. Confirmation should be provided certifying either on the photocopies sighted or the original documents or on the record of the evidence provided.

3.5. Concession-Payment by Post

3.5.1. Concession is granted for product or services where the money laundering risk is considered to be low, e.g. for long-term life insurance business or purchase of personal investment products. If a payment is to be made from an account held in the insured/ policyholder's name (or jointly with one or more other persons) at a regulated insurance company, no further evidence of identity is necessary.

3.5.2. Waiver of additional verification requirements for postal or electronic transactions does not apply to the following :

(*i*) Product or policy where claims/surrenders/funds can be transferred to other types of products or policy ;

(*ii*) Situation where claims/surrenders can be repaid or transferred to a person other than the original policyholder ;

(*iii*) Investments where the characteristics of the product or policy may change subsequently to enable payments to be made to third parties.

3.5.3. It should be noted that postal concession is not an exemption from the requirement to obtain satisfactory evidence of a policy holder's identity. Premium debited from an account in the policy holder's name shall be capable of constituting the required identification evidence in its own right.

3.5.4. To avoid criminal money being laundered by a policy holder for a third party, a cheque, draft or electronic payment drawn on a bank or other financial institutions may only be relied upon without further verification of identity where there is no apparent inconsistency between the name in which the policy is made and the name on the payment instrument. Payments from joint policy are considered acceptable for this purpose. The overriding requirement is that the name of the account holder from where the premiums have been provided is clearly indicated on any premium payment received.

3.5.5. In the case of a mortgage-backed policy, it will only be possible to rely on this concession if the mortgage institution can be confirmed to have met the KYP requirements.

3.5.6. In the case of policy transfer, record should be maintained indicating how a transaction arose, including details of the insurance company's branch and policy number from where the policy is transferred.

3.5.7. The concession can apply both where an application is made directly to the insurance company and where a payment is, for example, passed through a regulated intermediary.

3.5.8. An insurance company that has relied on the postal concession to avoid additional verification requirements (which must be so indicated on the policy holder's policy file) cannot introduce that policy holder to another insurance company for the purpose of offering or taking new policy or other products.

Deposit Administration (DA).

3.6.1. Deposit Administration can be broadly classified as a one-off transaction. However, insurance companies should note that concession is not available for DA's opened with cash where there is no audit trail of the source of funds or where deposit/withdrawal from third parties are allowed into the account. The identity verification requirements will therefore differ depending on the nature and terms of the DA.

Investment Linked Policy/DA.

3.7.1. In circumstances where the balance in an investment-linked policy/ DA is transferred from one insurance company to another and the value at that time is above ₦500,000 for an individual and ₦2,000,000 for a body corporate and if identification evidence has neither been taken nor confirmation obtained from the original insurance company, then such evidence should be obtained at the time of the transfer.

Establishment of Identity.

4.0. Establishing identity under this guidance note is divided into two broad categories :

(*i*) Identity for private individual policy holders ;

(*ii*) Identity for corporate policy holders (quasi and pure).

Private Individuals.

4.1.1. The following information should be established and independently validated for all private individuals whose identity needs to be verified :

(*i*) The true full name(s) used ; and

(*ii*) The permanent home address, including landmarks and postcode where available.

4.1.2. The information obtained should provide satisfaction that a person of that name exists at the address given and that the applicant is that person. Where an applicant has recently moved house, the previous address should be validated.

4.1.3. Date of birth is required by the law enforcement agencies and it is therefore important for this to be obtained. However, the information need not be verified. It is also important for the residence/nationality of a policy holder to be ascertained to assist risk assessment procedures.

4.1.4. A risk-based approach should be adopted when obtaining satisfactory evidence of identity. The extent and number of checks can vary depending on the perceived riskiness of the service or business sought and whether the application is made in person or through a remote medium, such as; telephone, post or the Internet. The source of funds, i.e. how the payment was made, from where and by whom, must always be recorded to provide an audit trail. However, for higher risk products, e.g. group/individual life policy holders, additional steps should be taken to ascertain the source of wealth/ funds.

4.1.5. For lower risk policy or simple investment products, e.g. DA, Investment Linked Policy, there shall be overriding requirements for the insurance company to satisfy itself as at the identity and address of the policy holder.

4.2.1. The confirmation of name and address should be established by reference to a number of sources. The checks should be undertaken by cross validation that the applicant exists at the state address either through the sighting of actual documentary evidence, or by undertaking electronic checks of suitable databases, or by a combination of the two. The overriding requirement to ensure that the identification evidence is satisfactory rests with the insurance company providing the product/service.

4.2.2. *Documentary Evidence of Identity.*—To guard against forged or counterfeit documents, care should be taken to ensure that documents offered are originals. Copies that are dated, signed, 'original seen' by a senior public servant or equivalent in a reputable private organization could be accepted in the interim pending presentation of the original documents.

4.2.3. *Documentary Evidence.*—Hereunder are example of suitable documentary evidence of Nigeria resident private individuals :

Private Individuals not Resident in Nigeria.

(*i*) Personal Identity Documents :

(*a*) Current International Passport ;

(*b*) Residence Permit issued by the Immigration Authorities ;

(*c*) Current Driving Licence issued by the Federal Road Safety Commission (FRSC) ;

(*d*) Tax Clearance Certificate ;

(*e*) Birth Certificate/Sworn Declaration of Age ;

(*f*) National Identity Card.

(*ii*) Documentary Evidence of Address :

(*a*) Policy certificate ;

(*b*) Record of home visit (non-Nigerians) ;

(*c*) Confirmation from the electoral registers that a person of that name lives at that address ;

(*d*) Recently utility bill (e.g. NEPA, NITEL, etc) ;

(*e*) State/Local Government Rates ;

(*f*) Current Driving Licence issued by FRSC ;

(*g*) Statement or Passbook containing current address ;

(*h*) Solicitor's letter confirming recent house purchase or Search Report from the Land Registry ;

(*i*) Tenancy Agreement ;

(*j*) Search Report on prospective policy holder's place of employment and residence signed by a senior officer of the insurance company ;

(*k*) Checking of a local or national telephone directory can be used as additional corroborative evidence, but should not be used as a primary check.

Physical Checks on Private Individuals Resident in Nigeria.

4.3.1. It is imperative for insurance companies systems to be capable of establishing the true identity and address of the policy holder and for effective checks to be in place to protect against the substitution of identity by an applicant.

4.3.2. Additional confirmation of the policy holder's identity and the fact that the application was made by the person identified should be obtained through one or more of the following procedures :

(*a*) Telephone contact with the applicant prior to delivery of policy Certificate on an independently verified residential address or business number, or a "welcome call" to the policy holder before transactions are permitted, utilizing minimum of two pieces of personal identity information that had been previously provided during the filling of the Proposal Form.

(*b*) Internet sign-on following verification procedures where the policy holder uses security codes, tokens, and/or other passwords which had been set up and provide by mail (or secure delivery) to the named individual at an independently verified address.

4.3.3. Care should be taken to ensure that any additional information required concerning the nature and level of the business to be conducted and the origin of the funds be used within the relationship, is also obtained from the policy holder.

Electronic Checks.

4.4.1. As an alternative or supplementary to documentary evidence of identity and address, the applicant's identity, address and other available information may be checked electronically by accessing other data sources. Each source may be used separately as an alternative to one or more documentary checks.

4.4.2. Care should be taken when using a combination of electronic and documentary checks that different original source of information are used. For example, a physical check of the policy documents and electronic check of the same document are the same source.

4.4.3. Some examples of suitable electronic sources of information are set out below :

(*a*) An electronic search of the Electoral Register (not to be used as a sole identity and address check) ;

(*b*) Access to internal or external database ;

(*c*) An electronic search of public records where available.

4.4.4. In addition to, or integral within, the above process and procedures should exist to guard against impersonation, invented identities and the use of false address. However, if the applicant is non-face to face, one or more additional measures should be undertaken.

4.4.5. The insurance company should satisfy itself, that a policy holder is the person he claims to be. Therefore, where a letter/statement is accepted from a professional person, it should include a telephone number where the person can be contacted for verification. The insurance company should verify from an independent source the information provided by the professional person.

4.4.6. To guard against exclusion and to minimize the use of the exception procedure, insurance companies must include in their internal procedures the alternative documentary evidence of personal identity and address that can be accepted.

4.4.7. Insurance companies should consider putting in place additional monitor for relationship opened under the financial exclusion exception procedures to ensure that such relationships are not misused.

Private Individuals Resident in Nigeria.

4.5.1. For those prospective policy holders who are not resident in Nigeria but who make face-to-face contact, international passports or national identity cards should generally be available as evidence of the name of the policy holder. Reference numbers, date, and country of issue should be obtained and the information recorded in the policy holder's file as part of the identifications evidence.

4.5.2. Insurance companies should obtain separate evidence of the applicant's permanent residential address from the best available evidence, preferably from an official source. A Post Office Box number alone will not normally be sufficient evidence of address. The applicant's residential address should be such that it can be physically located by way of a recorded description or other means.

4.5.3. The insurance company should obtain relevant evidence directly from the policy holder, or through a reputable institution in the applicant's home country or country of residence. However, particular care should be taken when relying on identification evidence provided from other countries to ensure that the policy holder's true identity and current permanent address has been confirmed. In such cases, copies of relevant identity documents should be sought and retained.

4.5.4. Where a foreign national has recently arrived in Nigeria, reference might be made to his/her employer, higher institutions attended, etc to verify the applicant's identity and residential address.

Supply of Information by post, Telephone, and Electronic Means (Private Individuals not Resident in Nigeria.

4.6.1. For a private individual not resident in Nigeria, who wishes to supply documentary information by post, telephone or electronic means, a risk-based approach must be taken. The insurance company should obtain one separate item of evidence of identity of the name of the policy holder and one separate item or the address.

4.6.2. Documentary evidence of name and address can be obtained :

(*a*) By way of original documentary evidence supplied by the policy holder ; or

(*b*) By way of a certified copy of the policy holder's passport or national identity card and a separate certified document verifying address e.g. a driving licence, utility bill, etc. ; or

(*c*) Through a branch, subsidiary, head office. Where the applicant does not already have a business relationship with the insurance company that is supplying the information, or the insurance company is not within Nigeria, certified copies of relevant underlying documentary evidence should be sought and retained in the institution.

Non Face-to-Face Identification.

4.6.3. Where necessary, additional comfort should be obtained by confirming the policy holder's true name, address and date of birth from a reputable credit institution in the policy holder's home country.

4.7.1. Because of possible false identities and impersonation that can arise with non face-to-face policy holders, it is important to ensure that the applicant is who he/she claims to be. Accordingly, one additional measure or check should be undertaken to supplement the documentary or electronic evidence. These additional measures must be particularly robust where the applicant is requiring a life policy or other product/service that offers money transmission or third party payments.

4.7.2. Procedures to identify and authenticate the policy holder should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity and to undertake at least one additional check to guard against impersonation.

4.7.3. The extent of the identification evidence required will depend on the nature and characteristics of the product or service and the assessed risk. However, care must be taken to ensure that the same level of information is obtained for Internet policy holders and other postal /telephone policy holders.

4.7.4. If reliance is being placed on intermediaries to undertake the processing of application on the policy holder's behalf, checks should be undertaken to ensure that the intermediary are regulated for money laundering prevention and that the relevant identification procedures are applied. In all cases, evidence as to how identity has been verified should be obtained and retained with the policy holder's records.

4.7.5. Insurance companies should consider regular monitoring of Internet base business/clients. If a significant proportion of the business is operated electronically, computerized monitoring systems that are designed to recognize unusual transactions and related patterns of transactions should be put in place for recognizing suspicious transaction. The Internal Audit Department should consider the use of CAATs (Policy Holder Audit Aided Tools) and other Information Systems Audit procedures and controls in the course of their work.

5.0. ESTABLISHING IDENTITY—PURE CORPORATE POLICY HOLDERS

General Principles.

5.1.1. Because of the complexity of their organizations and structures, corporate and legal entities are the most likely vehicles for money laundering, especially those that are private companies fronted by a legitimate trading company. Care should be taken to verify the legal existence of the applicant (i.e. the company) from official documents or sources and to ensure that any person purported to act on behalf of the applicant is fully authorized. Enquires should be made to confirm that the company is not merely a "*brass plate company*" where the controlling principals cannot be identified.

5.1.2. The identity of a corporate company comprises :

(*a*) Its registration number ;

(*b*) Its registered corporate name and any trading names used ;

(*c*) Its registered address and any separate principals trading addresses ; and

(*d*) Its directors ;

(*e*) Its owners and shareholder ; and

(*f*)The nature of the company's business.

Non Face-to-Face Business.

5.1.3. The extent of identification measures required to validate this information or the documentary evidence to be obtained depends on the nature of the business or service that the company requires from the insurance company. A risk-based approach should be taken. In all cases, information as to the nature of the normal business activities that the company expects to undertake with the insurance company should be obtained. Before a business relationship is established, measures should be taken by way of company search at the Corporate Affairs Commission (CAC) and/or other commercial enquiries to check that the applicant company has not been, or is not in the process of being dissolved, struck off, wound up or liquidated.

6.0.—(*i*) As with the requirements for private individuals, because of the additional risks with non face-to-face business, additional procedures must be undertaken to ensure that the applicant's business. company or society exists at the address provided and for a legitimate purpose.

(*ii*) Where the ch racteristics of the product or service permit, care should be taken to ensure that relevant evidence is obtained to confirm that any individual representing the company has the necessary authority to do so.

(*iii*) When principal owners, controllers or signatories need to be identified within the relationship, the relevant requirements for personal policy holders should be followed.

Procedures for Low Risks Corporate Business-Public Registered Company.

6.1.—(*i*) Corporate policy holders that are listed on the stock exchange are considered to be publicly owned and generally accountable. Consequently, there is no need to verify the identity of the individual shareholders.

(*ii*) Similarly, it is not necessary to identify the directors of a quoted company. However, insurance companies should make appropriate arrangements to ensure that the individual officer or employee (past or present) is not using the name of the company, or its relationship with the insurance companies for a criminal purpose. The Board Resolution or other authority for any representative to act on behalf of the company in its dealings with the insurance company should be obtained to confirm that the individual has the authority to act.

(*iii*) Consequently, where the applicant company is :

(*a*) Listed on the stock exchange ; or

(*b*) There is independent evidence to show that it is a wholly owned subsidiary or a subsidiary under the control of such a company ;

(*c*) No further steps to verify identity over and above the usual commercial checks and due diligence will normally be required, unless the business or service required falls within the category of high risk business.

Private Companies.

6.2.1. Where the applicant is an unquoted company and none of the principal directors or shareholders already had a policy with the insurance company, the following documents should be obtained from an official or recognized independent source to verify the business itself :

(*i*) A copy of the certificate of incorporation/registration; and evidence of the company's registered address and the list of shareholders and directors ; or

(*ii*) A search at the Corporate Affairs Commission (CAC) or an enquiry via a business information service to obtain the information in (*i*) ; or

(*iii*) An undertaking from a firm of lawyers or accountants confirming the documents submitted to the CAC.

6.2.2. Attention should be paid to the place of origin of the documents and the background against which they were produced. If comparable documents cannot be obtained, then verification of principal beneficial owners/controllers should be undertaken.

Additional Measure for Higher Risk Business Relating to Companies.

6.2.3. For private companies undertaking higher risk business, in addition to verifying the legal existence of the business, the principal requirement is to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets. What constitutes significant shareholding or control for this purpose will depend on the nature of the

company. Identification evidence will normally need to be obtained for those shareholders with interest of 5 per cent or more. Principal control rests with those who are mandated to manage funds, accounts or investments without requiring authorization and, who would be in a position to override internal procedures and control mechanisms.

6.2.4. Identification evidence should be obtained for the principal beneficial owner(s) of the company and any other person with principal control over the company's assets. Where the principal owner is another corporate entity or trust, the objective is to undertake measures that look behind that company or vehicle and verify the identity of the beneficial owner(s) or setters. When insurance companies become aware that principal beneficial owners/controllers have changed, care should be taken to ensure that their identities are verified.

6.2.5. Taking a risk base approach, insurance companies should identify directors who are not principal controllers and/or signatory to the policy holder.

6.2.6. In respect of a full insurance relationship, particularly where turnover is significant, a visit to the place of business should be undertaken to confirm the existence of business premises and the nature of the business activities conducted.

6.2.7. If suspicions are aroused by a change in the nature of the business transacted further checks should be made to ascertain the reason of the changes.

6.2.8. For full insurance relationship, periodic enquires should be made to establish whether there have been any changes to controllers /shareholders or to the original nature of the business/activity.

6.2.9.1. Particular care should be taken to ensure that full identification and "Know Your Policy Holder" requirements are met if the company is an International Business Company (IBC) registered in an offshore jurisdiction and operating out of a different jurisdiction.

6.3. Establishing Identity other Institutions

Establishing Identity– Clubs and Societies.

6.3.1. In the case of applications made on behalf of clubs or societies, an insurance company should take reasonable steps to satisfy itself as to the legitimate purpose of the organization by sighting its constitution. The identity of at least two of the principal contacts/ signatories should be verified initially in line with the requirements for private individuals. Signing authorities should be structured to ensure that at least one of the signatories authorizing any transaction has been verified. When signatories change, care should be taken to ensure that the identity of at least two of the current signatories is verified.

6.3.2. Where the purpose of the club/society is to purchase group life policies where all the members would be regarded as individual clients, all members should be identified in line with the requirements for personal policy holders. Insurance companies will need to look at each situation on a case-by-case basis.

Establishing Identity of Occupational Pension Schemes.

6.4.1. In all transactions undertaken on behalf of an Occupational Pension Scheme where the transaction is not in relation to a long-term policy of insurance, the identity of both the Principal Employer and the Trust should be verified.

6.4.2. In addition to the identity of the Principal Employer, the source of funding should be verified and recorded to ensure that a complete audit trail exists if the employer is dissolved /wound up.

6.4.3. For the Trustees of Occupational Pension Schemes, satisfactory identification evidence can be based on the inspection of formal documents concerning the trust which confirm the names of the current trustees and their address for correspondence. In addition to the documents, confirming the trust identification can be based on extracts from Public Registers, or references from Professional Advisers or Investment Managers.

6.4.4. Any payment of benefits by, or on behalf of the Trustees of an Occupational Pension Scheme will not require verification of identity of the recipient.

6.4.5. Where individual members of an Occupational Pension Scheme are to be given personal investment advice, their identities must be verified. However, where the Trustees and Principal Employer have been satisfactorily identified (and the information is still current), it may be appropriate for the Employer to provide confirmation of the identity of individual employees.

Religious Organizations (ROs).

7.1.1. A religious organization is expected by law to register with the Corporate Affairs Commission (CAC) and will therefore have a registered number. Its identity can be verified by reference to the CAC, appropriate headquarters or regional area of the denomination. As a registered organization, the identity of at least two signatories to its account should be verified.

Establishing Identity 3-Tiers of Government/ Parastatals and Educational Institutions.

8.1. Where the applicant for business is any of the above, the Insurance company should take steps to verify the legal standing of the applicant, including its principal ownership and address where applicable. A certified copy of the Resolution or other document authorizing the transaction should be obtained in addition to evidence that the official representing the body has the relevant authority to act. Telephone contact could also be made with the organization/ parastatals concerned.

9.0. Reliance on Intermediaries or other Third Parties to Verify Identity or to Introduce Business

Who can be relied upon and in what circumstances?

9.1.1. Whilst the responsibility to obtain satisfactory identification evidence rests with the insurance company that is entering into the relationship with a client/the insured, it is reasonable in a number of circumstances for reliance to be placed on another insurance company e.g. (Brokers) to :

(*a*) Undertake the identification procedure when introducing a policy holder and to obtain any additional KYP information from the client ; or

(*b*) Confirm the identification details if the policy holder is not resident in Nigeria ; or

(*c*) Confirm that verification of identity has been carried out, if an agent is acting for underlying principals.

9.1.2. Introductions from Authorised Insurance Intermediaries

9.1.3. Where an intermediary introduces a policy holder and then withdraws from the ensuing relationship altogether-the underlying policy holder is the applicant for business and must be identified in line with the requirements for personal, corporate or business policy holders as appropriate. An introduction letter should therefore be issued by the introducing insurance company or person in respect of each applicant for business to ensure that product providers can meet their obligations, and that satisfactory identification evidence has been obtained and will be retained for the necessary statutory period, each introduction letter must either be accompanied by certified copies of the identification evidence that has been obtained in line with the usual practice of certification of identification documents or by sufficient details/reference numbers, etc that will permit the actual evidence obtained to be re-obtained at a later stage.

9.1.4. Written Applications

9.1.5. For written business, unless other arrangements have been agreed that the service provider will verify identity itself, an insurance intermediary must provide along with each application, a policy holder introduction letter together with certified copies of the evidence of identity, which should be placed in the policy holder's file.

9.1.6. If these procedures are followed, the product provider, insurance company will be considered to have fulfilled its own identification obligations. However, if the letter is not forthcoming from the intermediary, or the letter indicates that the intermediary has not verified the identity of the applicant, the service provider will have to satisfy its obligation through its own direct identification procedures.

Non-Written Applications.

9.2.1. Product providers receiving non-written applications from insurance intermediaries, i.e. where a deal is placed over the telephone or by other electronic means, have an obligation to verify the identity of policy holders and, ensure that the intermediary provides specific confirmation that identity has been verified. A record must be made of the answers given by the intermediary and retained for the relevant period of 10 years. These answers constitute sufficient evidence of identity in the hands of the service provider.

Introductions from Foreign Intermediaries.

10.1. Where business introduced is from a regulated insurance intermediary who is outside Nigeria, the reliance that can be placed on that intermediary to undertake the verification of identity check must be assessed by the MLCO or some other competent person within the business on a case by case basis based on knowledge of the intermediary.

Corporate Group Introductions.

11.1. Where a policy holder is introduced by one part of an insurance sector to another, it is not necessary for identity to be re-verified or for the records to be duplicated provided that :

(*a*) The identity of the policy holder has been verified by the introducing parent company, branch, subsidiary or associate in line with the money laundering requirements, or to equivalent standards, and taking account of any specific requirements (e.g. separate address verification) ;

(*b*) No exemptions or concessions have been applied in the original verification procedures that would not be available to the new relationship;

(*c*) A group introduction letter is obtained and placed with the policy holder policy records ;

(*d*) In respect of group introducers from outside Nigeria, arrangements should be put in place to ensure that identity is verified in accordance with requirements and that the underlying records of identity in respect of introduced policy holders are retained for the necessary period.

11.2. Where insurance companies have day-to-day access to all group "*Know Your Policy Holder*" information and records, there is no need to identify an introduced policy holder, or obtain a group introduction letter, if the identity of that policy holder has been verified previously. However, if the identity of the policy holder has not previously been verified, then any missing identification evidence will need to be obtained and a risk-based approach taken on the extent of KYP information that is available and whether additional information should be obtained.

12.2. Insurance companies should ensure that there is no secrecy or data protection legislation that would restrict free access to the records on request, the regulator or by law enforcement agencies.

12.3. Where identification records are held outside Nigeria, it is still the responsibility of the insurance company to ensure that the records available do in fact meet the requirements in the guidelines.

Business Conducted by Agents.

13.1. Where an applicant is dealing in its own name as agent for its own client(s), an insurance company must, in addition to verifying the agent, establish the identity of the underlying client(s).

13.2. An insurance company may regard evidence as sufficient if it has established that the insured :

(*a*) Is bound by this guidelines or the Money Laundering Act No. 30, 1995 and as amended.

(*b*) Is acting on behalf of another person and has given a written assurance that he has obtained and recorded evidence of the identity of the person on whose behalf he is acting.

13.3. Consequently, where another Insurance company deals for its own client, regardless of whether the underlying client is disclosed to the Insurance company or not, then :

(*a*) Where the intermediary is an Insurance company, there is no requirement to establish the identity of the underlying clients or to obtain any form of written confirmation from the agent concerning the due diligence undertaken on its underlying clients : or

(*b*) Where a regulated agent from outside Nigeria, deals through a policy holder omnibus policy, or for a named policy holder through a designated policy, the intermediary should provide a written assurance, that the identity of all underlying insured has been verified in accordance with their local requirements. Where such an assurance cannot be obtained, then the business should not be undertaken.

13.4. In circumstances where an intermediary is either unregulated or is not covered by the relevant Money Laundering Legislation, then each case should be treated on its own merits depending on the knowledge of the agent and its due diligence standards.

Correspondent Relationship.

14.1. Transactions conducted through correspondent relationships need to be managed taking a risk-based approach. "Know Your Correspondent" procedures should be established to ascertain whether the correspondent institution or counter-party is itself regulated for money laundering prevention and, if so, whether the correspondent is required to verify the identity of its policy holders to FATF standards. Where this is not the case, additional due diligence will be required to ascertain and assess the correspondent's internal policy on money laundering prevention and it is know your policy holder procedures.

14.2. The volume and nature of policy flowing through correspondent institution with insurance companies from high risk jurisdictions or those with inadequacies or material deficiencies should be monitored against expected levels and destinations and any material variances should be checked.

14.3. Insurance companies should guard against passing funds through their accounts without taking reasonable steps to satisfy themselves that sufficient due diligence has been undertaken by the remitting bank on the underlying client and the origin of the funds.

14.4. Insurance companies should also guard against establishing correspondent relationships with high-risk foreign, Reinsurers insurers/ intermediaries e.g. Shell Insurance broker with no physical presence in any country.

14.5. Staff dealing with correspondent Insurance business should be trained to recognize higher risk circumstances and be prepared to challenge correspondents over irregular activity, where isolated transactions or trends, and submit a suspicious activity report where appropriate.

14.6. Local insurance companies should consider terminating their policy with foreign insurers insurance company that fail to provide satisfactory answers to reasonable questions including confirming the identity of policy holders involved in unusual or suspicious circumstances.

Acquisition of one Insurance Company or Business by Another.

15.1. When an insurance company acquires the business of another firm, it is not necessary for the identity of all existing policy holders to be re-identified, provided that all underlying policy holder records are acquired with the business. It is however important for the due diligence enquiries to confirm that the acquired institution conformed to the requirements in this guidelines.

15.2. In the event that :

(*a*) The money laundering procedures previously undertaken have not been in accordance with the requirements of this guidelines ; or

(*b*) The procedures cannot be checked ; or

(*c*) Where the policy holder records are not available to the acquiring insurance company.

(*d*) Verification of identity should be undertaken as soon as it is practicable for all the transferred policy holders who were not verified by the transferee in line with the requirements for existing policy holders.

Exemption from Identification Procedures.

16.1. All insurance companies shall establish policy holder identity in line with the contents of these guidelines except where applicants are Nigerian Insurance companies. Identification evidence is not required where the

applicant for business is a Nigerian person or firm that is covered by the requirements of these guidelines.

17.0. Failure to comply with the provisions of this guidelines will attract appropriate sanction in accordance with existing laws.

Actions for Non-Compliance.