United Republic of Tanzania

Financial Intelligence Unit

Anti-Money Laundering and Counter-Terrorist Financing

Guidelines to Insurers

GUIDELINES NO: 4

TABLE OF CONTENTS

ACRONYMS

AML	Anti Money Laundering
AML Act	Anti Money Laundering Act, 2006
BoT	Bank of Tanzania
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CMSA	Capital Markets and Securities Authority
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IAIS	International Association of Insurance Supervisors
ML	Money Laundering
PEP	Politically Exposed Person
TIRA	Tanzania Insurance Regulatory Authority
TZS	Tanzanian Shillings
UN	United Nations
UNSCR	United Nations Security Council Resolution

1 INTRODUCTION

1.1 The Anti-Money Laundering Act, 2006 was promulgated to make better provisions for the prevention and prohibition of money laundering, to provide for the disclosure of information on money laundering, to establish a Financial Intelligence Unit and the National Multi-Disciplinary Committee on Anti-Money Laundering and to provide for matters connected thereto.

1.2 These guidelines are issued pursuant to Section 6(f) of the Anti-Money Laundering Act, 2006 and Regulation 32 (1) 9 (c) of the Anti-Money Laundering Regulations, 2007. The guidelines apply to all insurers (offering life or non-life products) operating in Tanzania.

1.3 The ability to launder the proceeds of crime through the financial system is vital for the success of criminals. Those involved need to exploit the facilities of the world's financial institutions such as banks, insurance companies and securities firms, if they are to benefit from the proceeds of their illegal activities. The increased integration of the world's financial systems, and the removal of barriers to the free movement of capital, goods and services have enhanced the ease with which proceeds of crime can be laundered and have complicated the tracing and tracking process.

1.4 The International Association of Insurance Supervisors (IAIS), a body which represents insurance regulators and supervisors of some 190 jurisdictions, noted that the insurance sector, like other sectors of the financial services industry, are potentially at risk of being misused for money laundering and the financing of terrorism. Criminals look for ways of concealing the illegitimate origin of funds. Persons involved in organizing terrorist acts look for ways to finance these acts. The products and transactions of insurers can provide the opportunity to launder money or to finance terrorism. The vulnerability depends on factors such as (but not limited to) the complexity and terms of the contract, distribution, method of payment (cash or bank transfer) and contract law. Some examples of the type of life insurance contracts that are vulnerable as a vehicle for laundering money or terrorist financing are products such as:

- unit-linked or with profit single premium contracts

- single premium life insurance policies that store cash value
- fixed and variable annuities, and
- (second hand) endowment policies.

More examples of money laundering or suspicious transactions involving insurance are given at Appendix A.

1.5 Insurers can be involved, knowingly or unknowingly, in money laundering and the financing of terrorism. This exposes them to legal, operational and reputational risks. The insurance sector should therefore take adequate measures to prevent its misuse by money launderers and terrorists.

2 CUSTOMER DUE DILIGENCE (CDD)

2.1 Anonymous Account of Fictitious Persons

No insurer shall deal with any person on an anonymous basis or any person using a fictitious name.

2.2 When CDD is to be performed

An insurer shall perform CDD measures when –

(a) the insurer establishes business relations with any customer

(b) there is a suspicion of money laundering or terrorist financing, notwithstanding that the insurer would otherwise not be required by this set of Guidelines to perform CDD measures, or

(c) the insurer has doubts about the veracity or adequacy of any information previously obtained.

2.3 Identification of Customers and Beneficial Owners and Verification of their Identities

(I) Identification of Customers

2.3.1 An insurer shall identify each customer who applies to the insurer to establish business relations.

2.3.2 For the purpose of paragraph 2.3.1 above, an insurer shall obtain and record information of the customer in accordance with the AML Act, including but not limited to the following:

(a) Full name, including any aliases

(b) Unique identification number (such as an identity card number, birth certificate number, voters registration card number, driving license number, national ID number, number on introduction letter from the local government executive, passport number or where the customer is not a natural person, the incorporation number or business registration number)

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s)

(d) Date of birth, incorporation or registration (as may be appropriate), and

(e) Nationality or place of incorporation or registration (as may be appropriate).

2.3.3 Where the customer is a company, the insurer shall, apart from identifying the customer, also identify the directors of the company.

2.3.4 Where the customer is a partnership or a limited liability partnership, the insurer shall, apart from identifying the customer, also identify the partners.

2.3.5 Where the customer is any other body corporate or unincorporate, the insurer shall, apart from identifying the customer, also identify the persons having executive authority in that body corporate or unincorporate.

(II) Verification of Identity

2.3.6 An insurer shall verify the identity of the customer using reliable, independent sources.

2.3.7 An insurer shall retain copies of all reference documents used to verify the identity of the customer.

2.4 Identification of Beneficial Owners and Verification of their Identity

2.4.1 An insurer shall inquire if there exists any beneficial owner in relation to a customer. "Beneficial owner", in relation to a customer of an insurer, means the natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a body corporate or unincorporate.

2.4.2 Where there is one or more beneficial owners in relation to a customer, the insurer shall take reasonable measures to obtain information sufficient to identity and verify the identity of the beneficial owner(s).

2.4.3 Where the customer is not a natural person, the insurer shall take reasonable measures to understand the ownership and structure of the customer.

2.4.4 An insurer shall not be required to inquire if there exists any beneficial owner in relation to a customer that is –

(a) a Tanzanian government entity

(b) a foreign government entity, provided it is not sanctioned or blacklisted by the international community such as the United Nations and FATF

(c) an entity listed on the stock exchange in Tanzania

(d) an entity listed on a stock exchange outside of Tanzania that is subject to adequate regulatory disclosure requirements (referred regulator should be a registered member of any International Association of Regulators)

(e) a financial institution supervised by the Bank of Tanzania, the CMSA or the TIRA

(f) a financial institution incorporated or established outside Tanzania that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF

(g) Life insurance policies where the annual premium is not more than TZS 1,500,000 or EURO/USD 1000 or a single premium of no more than TZS 4,000,000 or EURO/USD 2500

(h) Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral

(i) A pension, superannuation or similar scheme that provides retirement benefits 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

Unless the insurer suspects that the transaction is connected with money laundering or terrorist financing.

For the purposes of items (d) and (f) above, an insurer shall document the basis for its determination that the requirements in those paragraphs have been duly met.

2.5 Identification and Verification of Identity of Natural Persons Appointed to Act on Customer's Behalf

2.5.1 Where a customer appoints one or more natural persons to act on his behalf in establishing business relations with the insurer or the customer is not a natural person, an insurer shall-

(a) identify the natural persons that act or are appointed to act on behalf of the customer, as if such persons were themselves customers

(b) verify the identity of these persons using reliable, independent sources, and

(c) retain copies of all reference documents used to verify the identity of these persons.

2.5.2 In the case of private trusts, an insurer shall verify the authorization given to each trustee of the relevant trust.

2.5.3 An insurer shall verify the due authority of such person to act on behalf of the customer, by obtaining, including but not limited to, the following:

(a) the appropriate documentary evidence that the customer has appointed the persons to act on its behalf, and

(b) the specimen signatures of the persons appointed.

2.5.4 Where the customer is a Tanzanian government entity, the insurer shall only be required to obtain such information as may be required to confirm that the customer is a Tanzanian government entity as indicated.

2.6 Identification and Verification of Identity of Payee

2.6.1 Where the payee of the insurance policy is not a customer, an insurer shall identify the payee and verify his identity before making any of the following types of payment:

(a) payment of the sum assured (or part thereof) upon the occurrence of the risk insured against in accordance with the policy

(b) payment of the surrender value of the insurance policy

(c) refund of premium upon the avoidance, cancellation and/or termination of any insurance policy, or

(d) refund of any other payment made in relation to any insurance policy.

2.7 Information on the Purpose and Intended Nature of Business Relations

An insurer shall obtain, from the customer, when processing the application to establish business relations, information as to the purpose and intended nature of business relations.

2.8 Existing Customers

2.8.1 An insurer shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.

2.9 Reliance on Identification and Verification Already Performed

When an insurer ("acquiring insurer") acquires, either in whole or in part, the business of another financial institution (whether in Tanzania or elsewhere), the acquiring insurer shall perform CDD measures on customers acquired with the business at the time of acquisition except where the acquiring insurer has:

(a) acquired at the same time all corresponding customer records (including customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired, and

(b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring insurer as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring insurer.

2.10 Joint Account

2.10.1 In the case of a joint account, an insurer shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the insurer.

2.11 CDD Measures for Non-Policy Holders

2.11.1 An insurer that undertakes any transaction with a non-policy holder shall:

(a) establish and verify the identity of the customer as if the customer had applied to the insurer to establish business relations; and

(b) record adequate details of the transaction so as to permit the reconstruction of the transaction, including the nature and date of the transaction, the type and amount of currency involved, the value date, and the details of the payee.

2.12 Timing for Verification

An insurer shall complete verification of the identity of the customer and beneficial owner:

(a) before the insurer establishes business relations, or

(b) before the insurer undertakes any transaction for a customer, where the customer does not have business relations with the insurer.

2.12.1 An insurer may establish business relations with a customer before completing the verification of the identity of the customer and beneficial owner if:

(a) the deferral of completion of the verification of the identity of the customer and beneficial owner is essential in order not to interrupt the normal conduct of business operations, and

(b) the risks of money laundering and terrorist financing can be effectively managed by the insurer.

In all 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.

2.12.2 Where the insurer establishes business relations before verification of the identity of the customer or beneficial owner, the insurer shall complete such verification as soon as is reasonably practicable.

2.13 Where CDD Measures are Not Completed

2.13.1 Where the insurer is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of a suspicious transaction report (STR).

3 ENHANCED DUE DILIGENCE - POLITICALLY EXPOSED PERSONS

3.1 An insurer shall, in relation to politically exposed persons (as defined in the AML Act), perform enhanced CDD measures in addition to normal CDD measures, including but not limited to the following:

(a) implement appropriate internal policies, procedures and risk management systems to determine if a customer or beneficial owner is a politically exposed person

(b) obtain approval from the insurer's senior management to establish or continue business relations where the customer or beneficial owner is a politically exposed person or subsequently found to be or subsequently becomes a politically exposed person

(c) take reasonable measures to establish the source of wealth and source of funds of the customer or beneficial owner, and

(d) conduct, during the course of business relations, enhanced monitoring of business relations with the customer.

4 ENHANCED DUE DILIGENCE - OTHER HIGHER RISK CATEGORIES OF CUSTOMERS

4.1 An insurer shall perform enhanced CDD measures in paragraph 3 for such other categories of customers, business relations or transactions as the insurer may assess to prevent a higher risk for money laundering and terrorist financing.

4.2 An insurer shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the insurer for itself or notified to insurers generally by the FIU or other foreign regulatory authorities.

5 MEASURES TO ADDRESS USE OF NEW TECHNOLOGIES AND NON-FACE-TO-FACE BUSINESS VERIFICATION

5.1 An insurer shall put in place policies and procedures to address any specific risks associated with the use of new technologies and non-face-to-face business relations or transactions.

5.2 An insurer shall implement the policies and procedures referred to in paragraph 5.1 when establishing customer relationships and when conducting ongoing due diligence.

5.3 Where there is no face-to-face contact, the insurer shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

6 RELIANCE ON INTERMEDIARIES TO PERFORM CDD MEASURES

6.1 An insurer may rely on an intermediary to perform CDD measures in accordance with the Law and regulations if the following requirements are met:

(a) the insurer is satisfied that the intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements

(b) the intermediary is not one on which insurers have been specifically precluded by relevant Tanzanian authorities from relying

(c) the intermediary is able and willing to provide, without delay, upon the insurer's request, any document obtained by the intermediary which the insurer would be required or would want to obtain, and .

(d) the intermediary has capacity in terms of competent staff and resources to carry out CDD

6.2 No insurer shall rely on an intermediary to conduct ongoing monitoring of customers.

6.3 Where an insurer relies on an intermediary to perform the CDD measures, it shall:

(a) document the basis for its satisfaction that the requirements in paragraph 6.1a have been met, and

(b) immediately obtain from the intermediary the information relating to CDD measures obtained by the intermediary.

6.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the insurer shall remain responsible for its AML/CFT obligations as required under the Law , Regulations and Guidelines.

7 RECORD KEEPING

7.1 Every reporting person shall prepare, maintain and retain documentation on all its business relations, transactions (these include account files and business correspondences) with its customers such that –

(a) all requirements imposed by the AML Act and Regulations are met

(b) any transaction undertaken by the reporting entity can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal/money laundering activity

(c) the relevant competent authorities in Tanzania and the internal and external auditors of the reporting entity are able to review the entity's transactions and assess the level of compliance with the law and regulations, and

(d) the reporting entity can make available records on a timely basis to domestic competent authorities upon appropriate authority for information.

7.2 A reporting entity shall, when setting its record retention policies and performing its internal procedures, comply with the following document retention periods:

(a) a period of at least five years following the termination of business relation for customer identification document, and other documents relating to the establishment of business relations, as well as account files and business correspondence, and

(b) a period of five years following the completion of transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

These document retention periods are subject to paragraph 7.3.

7.3 A reporting entity shall retain records pertaining to a matter which is under investigation or which has been the subject of a suspicious transaction report (STR) for such longer period as may be necessary in accordance with any request or order from relevant competent authorities in Tanzania.

8 ONGOING MONITORING AND PAYING ATTENTION TO UNUSUAL TRANSACTIONS

8.1 An insurer shall monitor on an ongoing basis, its business relations with customers.

8.2 An insurer shall, during the course of business relations, observe the conduct of the customer's policy and scrutinize transactions undertaken to ensure that the transactions are consistent with the insurer's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

8.3 An insurer shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

8.4 An insurer shall take reasonable steps to inquire into the background and purpose of the transactions in paragraph 8.3 and document such information and its findings. The

9 ENSURING CUSTOMER INFORMATION IS KEPT UP-TO-DATE

9.1 An insurer shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers.

10 SUSPICIOUS TRANSACTION REPORTING

10.1 An insurer shall keep in mind the provisions of subsection (1) of Section 17 of the AML Act, Cap 423 and Regulation 20 (1) and (2) of the Anti-Money Laundering Regulation 2007 that provide for reporting to competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to the FIU and

(b) keep records of all transactions referred to the FIU, together with all internal findings and analysis done in relation to them.

10.2 An insurer shall submit reports on suspicious transactions (including attempted transactions) to the Tanzania FIU.

10.3 An insurer shall consider if the circumstances are suspicious so as to warrant the filing of a suspicious transaction report and document the basis for its determination where:

(a) the insurer is for any reason unable to complete CDD measures, or

(b) the customer is reluctant, unable or unwilling to provide any information requested by the insurer, decides to withdraw a pending application to establish

business relations or a pending transaction, or to terminate existing business relations.

11 INTERNAL POLICIES, COMPLIANCE, AUDIT, TRAINING AND EMPLOYEE/AGENT SCREENING

11.1 An insurer shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees and agents.

11.2 The policies, procedures and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and/or suspicious transactions and the obligation to make suspicious transaction reports.

11.3 In formulating its policies, procedures and controls, an insurer shall take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favor anonymity.

11.4 An insurer shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT officer. The insurer shall ensure that the AML/CFT officer, as well as any other persons appointed to assist him, have timely access to all customer records and other relevant information which they require to discharge their functions.

11.5 An insurer shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the insurer's internal policies, procedures and controls, and its compliance with regulatory requirements.

11.6 An insurer shall have in place screening procedures to ensure high standards when hiring employees and agents.

11.7 An insurer shall take all appropriate steps to ensure that its staff and agents (whether in Tanzania or overseas) are regularly trained on-

(a) AML/CFT laws and regulations, and in particular, CDD measures detecting and reporting suspicious transactions

(b) prevailing techniques, methods and trends in money laundering and terrorist financing, and

(c) the insurer's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff and agents in combating money laundering and terrorist financing.

12 FOREIGN BRANCHES AND SUBSIDIARIES

12.1 An insurer that is incorporated in Tanzania shall develop a group policy on AML/CFT and extend this to all its branches and subsidiaries where applicable outside Tanzania.

12.2 Where an insurer has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the insurer for itself or notified to insurers generally by the FIU/TIRA or by other relevant local or foreign authorities), the insurer shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

12.3 Where the AML/CFT requirements in the host country or jurisdiction differ from those in Tanzania, the insurer shall require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

12.4 Where the law of the host country or jurisdiction conflicts with Tanzania Law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the insurer's head office shall report this to the FIU/TIRA and comply with such further directions as may be given by the Authority.

13 EFFECTIVE DATE

These guidelines shall become effective on 1st April, 2011.

Herman M. Kessy

Commissioner

Financial Intelligence Unit

APPENDIX

EXAMPLES OF MONEY LAUNDERING/TERRORIST FINANCING INVOLVING INSURANCE

This appendix contains examples of money laundering or suspicious transactions involving insurance as compiled by the International Association of Insurance Supervisors (IAIS) and the Financial Intelligence Unit. These indicators are not exhaustive. It should be noted that none of these indicators on their own necessarily mean that a customer/policy holder or any third party is involved in any money laundering or terrorist financing. However, in most circumstances a combination of some of the following indicators should arouse suspicion. In any event, what does or does not give rise to a suspicion will depend on the particular circumstances.

Examples of money laundering/terrorist financing involving insurance

- Application for a policy from a potential client in a distant place where a comparable policy could be provided "closer to home".
- Application for business outside the policyholder's normal pattern of business.
- Introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where organised criminal activities (e.g. drug trafficking or terrorist activity) or corruption are prevalent.
- Any want of information or delay in the provision of information to enable verification to be completed.
- An atypical incidence of pre-payment of insurance premiums.
- The client accepts very unfavourable conditions unrelated to his or her health or age.
- The transaction involves use and payment of a performance bond resulting in a cross-border payment (wire transfers) and the first (or single) premium is paid from a bank account outside the country.
- Large fund flows through non-resident accounts with brokerage firms.

- Insurance policies with premiums that exceed the client's apparent means.
- The client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment.
- Insurance policies with values that appear to be inconsistent with the client's insurance needs.
- The client conducts a transaction that results in a conspicuous increase of investment contributions.
- Any transaction involving an undisclosed party.
- Early termination of a product, especially at a loss, or where cash was tendered and/or the refund cheque is to a third party.
- A transfer of the benefit of a product to an apparently unrelated third party.
- A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy).
- Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policyholder.
- Requests for a large purchase of a lump sum contract where the policyholder has usually made small, regular payments.
- Attempts to use a third party cheque to make a proposed purchase of a policy.
- The applicant for insurance business shows no concern for the performance of the policy but much interest in the early cancellation of the contract.
- The applicant for insurance business attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments.

- The applicant for insurance business requests to make a lump sum payment by a wire transfer or with foreign currency.
- The applicant for insurance business is reluctant to provide normal information when applying for a policy, providing minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify.
- The applicant for insurance business appears to have policies with several institutions.
- The applicant for insurance business purchases policies in amounts considered beyond the customer's apparent means.
- The applicant for insurance business establishes a large insurance policy and within a short time period cancels the policy, requests the return of the cash value payable to a third party.
- The applicant for insurance business wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.
- The applicant for insurance business use a mailing address outside the insurance supervisor's jurisdiction and where during the verification process it is discovered that the home telephone has been disconnected.

Examples of Suspicious Transactions Involving Cash Payments, Reluctance to Provide Information, Employees and Agents/Intermediaries

- Reluctance to provide normal information when establishing business relations, providing minimal or fictitious information or, when establishing business relations, providing information that is difficult or expensive for the institution to verify.
- Customers who decline to provide information that in normal circumstances would make the customer eligible for services that would be regarded as valuable.

- Customers introduced by an overseas branch, affiliate or other financial institution based in countries where production of drugs or drug trafficking may be prevalent.
- Customers who make regular and large payments, including wire transfers, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from countries which are commonly associated with the production, processing or marketing of drugs and proscribed terrorist organizations.
- Changes in employee characteristics (e.g. lavish lifestyles or avoiding taking holidays).
- Changes in employee or agent performance (e.g. the salesman selling products for cash has a remarkable or unexpected increase in performance).
- Any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, contrary to normal procedure for the type of business concerned.
- Intermediaries – There are clearly many legitimate reasons for a client's use of an intermediary. However, the use of intermediaries does introduce further parties into the transaction thus increasing opacity and depending on the designation of the account, preserving anonymity. Likewise, there are a number of legitimate reasons for dealing with via intermediaries. However, this is also a useful tactic, which may be used by the money launderer or terrorist financier to delay, obscure or avoid detection. Any apparently unnecessary use of an intermediary in the transaction should give rise to further enquiry.
- The excessive or unnecessary use of nominees.
- The unnecessary granting of wide ranging Powers of Attorney.
- An unwillingness to disclose the sources of funds.
- The use of a mailing address for non-residents.
- The tardiness and/or unwillingness to disclose the identity of the ultimate beneficial owners or beneficiaries.