RULES ON
KNOW YOUR CUSTOMER (KYC) & CUSTOMER DUE DILIGENCE (CDD)
FOR THE INSURANCE INDUSTRY

Introduction

Money laundering and terrorist financing can harm the soundness of a countryôs financial system, as well as the stability of individual institutions, in multiple ways. Customer identification and due diligence procedures also known as ñknow your customerò rules, are part of an effective Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) regime. These rules are not only consistent with, but also enhance, the safe and sound operation of insurance sector institutions.

While preparing operational guidelines on customer identification and due diligence procedures, institutions are advised to treat the information collected from the customer for the purpose of entering into insurance contracts, as confidential and not divulge any details thereof for cross-selling or for any other purposes, and that the information sought is relevant to the perceived risk, is not intrusive and is in conformity with the rules issued hereunder.

The rules on KYC/CDD include the following sections:

Part I - Role of the Supervisor
Part II - Money Laundering and Financing of Terrorism in insurance
Part III - Control Measures and Procedures against Money Laundering and Financing of Terrorism
Part IV - Anti-Money Laundering Programme
Part V - Suspicious Transaction Report, Instructions and Format.

These rules are issued under Section 2(3) of the Financial Transactions Reporting Act No.6 of 2006 and any contravention of, or non-compliance with the same will be liable to the penalties under the relevant provisions of the Act.

Director
Financial Intelligence Unit

Part I - Role of the Supervisor

1. Supervisory authority, in conjunction with law enforcement authorities and in cooperation with other supervisors, must adequately supervise insurers for anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) purposes in order to assess their ability to prevent and counter such threats.

Application of relevant insurance core principles

2. According to the International Association of Insurance Supervisors (IAIS) Insurance Core Principles a sound regulatory and supervisory system is necessary for maintaining efficient, safe, fair and stable insurance markets. The Financial Actions Task Force (FATF) Recommendations emphasise that jurisdictions should ensure that financial institutions are subject to adequate regulation and supervision, and are effectively implementing the FATF Recommendations. According to FATF Recommendation 23, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for AML/CFT.

3. Therefore, the supervisor should be aware of the relevance for AML/CFT purposes of the duties it carries out to comply with the Insurance Core Principles. By way of example, the application of standards on corporate governance issues; approval of control and ownership of the insurer and changes thereto; suitability of significant owners, board members and senior management (fit and proper testing; and the internal control measures of the insurers are relevant in this context.

4. Attention to money laundering and the financing of terrorism with respect to supervisory duties will enhance international efforts to prevent the risks of misuse of insurers. It will raise the awareness of the board of directors and management of insurers, help in keeping internal procedures effective, and prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in an insurer.

5. The supervisor should take account of these risks at each phase of the supervisory process, at the licensing stage and in the course of ongoing supervision.

6. The supervisory authority should have adequate powers, including the authority to conduct on-site inspections, to monitor and ensure compliance by insurers with requirements to prevent money laundering and the financing of terrorism. It should be authorised to compel production of any information from insurers that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.

7. The supervisor should periodically review the effectiveness of its systems to prevent money laundering and the financing of terrorism. This review may include liaison with other competent authorities.

8. The supervisor should be provided with adequate financial, human and technical resources to prevent or assess the insurance sectorôs ability to prevent money laundering and the financing of terrorism. It should have in place processes to ensure its staff are of high integrity and have adequate and relevant training for example with respect to AML/CFT legislation, money laundering and terrorist financing typologies and techniques used to monitor compliance with AML/CFT standards by insurers.

Monitoring compliance

9. The supervisor should monitor adherence by insurers with AML/CFT regulations, this guidance paper and any guidance issued by the supervisor as well as policy and procedures set by management.

10. When conducting on-site inspections the supervisor should consider the insurerôs policies and systems as a whole, inter alia by checking policy statements, procedures, books and records, manuals, training programmes, as well as the adequacy of operations, by checking at random or on a risk basis client files for identification and verification documentation, internal reports to the compliance officer on suspicious transactions and formal Suspicious Transaction Reports (STRs) to the Financial Intelligence Unit (FIU).

11. The supervisor should take appropriate corrective measures or sanctions and, if appropriate, refer to law enforcement agencies in cases where there is a lack of compliance by an insurer.

Cooperation

12. FATF Recommendation 31 states that jurisdictions should ensure that policy makers, the FIU, law enforcement agencies and supervisors have effective mechanisms in place which enable them to cooperate and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to prevent money laundering and the financing of terrorism.

13. FATF Recommendation 40 states that jurisdictions should ensure that their competent authorities, including the supervisors, provide the widest possible range of international cooperation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences.

14. FATF Recommendation 40 states that exchange of information should be permitted without unduly restrictive conditions. In particular:

- Å the competent authorities, including the supervisor, should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters,
- Å countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide cooperation,
- Å the competent authorities, including the supervisor, should be able to conduct inquiries and, where possible, investigations on behalf of foreign counterparts,

15. The supervisor should establish controls and safeguards so that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

16. Depending on the type of competent authorities involved and the nature and purpose of the cooperation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include bilateral or multilateral agreements or arrangements, memorandum of understanding, exchanges on the basis of reciprocity, or liaison through appropriate international or regional organizations.

Part II - Money Laundering and Financing of Terrorism in Insurance

The process of money laundering and financing of terrorism

1. Money laundering is the processing of the proceeds of crime to disguise their illegal origin. Once these proceeds are successfully ólaunderedô the criminal is able to enjoy these monies without revealing their original source. Money laundering can take place in various ways.

2. Financing of terrorism can be defined as the willful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds should be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts. Terrorism can be funded from legitimate income.

Vulnerabilities in insurance

3. Life insurance and non-life insurance can be used in different ways by money launderers and terrorist financiers. 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. Insurers should take these factors into account when assessing this vulnerability. This means they should prepare a risk profile of the type of business in general and of each business relationship.

4. 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

5. When a life insurance policy matures or is surrendered, funds become available to the policyholder or other beneficiaries. The beneficiary to the contract may be changed possibly against payment, before maturity or surrender, in order that payments are made by the insurer to a new beneficiary. A policy might be used as collateral to purchase other financial instruments. These investments in themselves may be merely one part of a sophisticated web of complex transactions with their origins elsewhere in the financial system.

6. Non-life insurance money laundering or terrorist financing can be seen through inflated or totally bogus claims, e.g. by arson or other means causing a bogus claim to be made to recover part of the invested illegitimate funds. Other examples include cancellation of policies for the return of premium by an insurerôs cheque, and the overpayment of premiums with a request for a refund of the amount overpaid. Money laundering can also occur through under-insurance, where a criminal can say that he received compensation for the full amount of the damage, when in fact he did not.

   Examples of how terrorism could be facilitated through property and casualty coverage, include use of workerôs compensation payments to support terrorists awaiting assignment and primary coverage and trade credit for the transport of terrorist materials.

7. Money laundering and the financing of terrorism using reinsurance could occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, fronting arrangements and captives, or by the misuse of normal reinsurance transactions. Examples include:

   - the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds,
   - the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding,
   - the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers.

8. Insurance intermediaries independent or otherwise are important for distribution, underwriting and claims settlement. They are often the direct link to the policyholder and therefore intermediaries should play an important role in anti-money laundering and combating the financing of terrorism. The FATF recommendations allow insurers, under strict conditions, to rely on customer due diligence carried out by intermediaries. The same principles that apply to insurers should generally apply to insurance intermediaries. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of, or does not conform to, necessary procedures, or who fails to recognise or report information regarding possible cases of money laundering or

the financing of terrorism. The intermediaries themselves could have been set up to channel illegitimate funds to insurers. In addition to the responsibility of intermediaries, customer due diligence ultimately remains the responsibility of the insurer involved.

Part III - Control Measures and Procedures against Money Laundering and Financing of Terrorism

1. Insurers should be constantly vigilant in deterring criminals from making use of them for the purposes of money laundering or the financing of terrorism. By understanding the risks of money laundering and the financing of terrorism, insurers are in a position to determine what can be done to control these risks, and which procedures and measures can be implemented effectively and efficiently.

2. For reasons of sound business practice and proper risk management insurers should already have controls in place to assess the risk of each business relationship. As customer due diligence is a business practice suitable not just for commercial risk assessment and fraud prevention but also to prevent money laundering and the financing of terrorism, control measures should be linked to these existing controls. The concept of customer due diligence goes beyond the identification and verification of only the policyholder which extends to identification of the potential risks of the whole business relationship.

3. The duty of vigilance consists mainly of the following elements:
   - customer due diligence, including underwriting checks and verification of identity,
   - recognition and reporting of suspicious customers/transactions, and
   - provisions affecting the organization and the staff of the insurer, such as a compliance and audit environment, keeping of records, the recruitment of staff and training.

Performing due diligence on customers, beneficial owners and beneficiaries

4. Insurers should know the customers[1] with whom they are dealing. A 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 insurer, including policies on products, markets and clients.

5. The insurerôs strategic policies will determine its exposure to risks such as underwriting risk, reputational risk, operational risk, concentration risk[2] and legal risk. After determining the strategic policies, client acceptance policies should be established, taking account of risk factors such as the background and

1 Under normal conditions the term ‘customer’ refers to ‘policyholder’.

2 Concentration risk: the risk that too much business is being conducted with persons or corporations belonging to the same conglomerate, group or geographical area.

geographical base of the customer and/or beneficial owner[3] and the complexity of the business relationship. This is why, as indicated above, control measures and procedures with respect to AML/CFT should be an integral part of the overall customer due diligence.

6. Insurers should be aware that, for example, 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 calls for more intensive checks on the background of the client and the origin of the premium than the latter. Insurers should also be aware of requests for multiple policies to be taken out for premiums slightly below any publicised limits for performing checks, such as checks on the source of wealth.

7. Customer due diligence measures that should be taken by insurers include:

- identifying the customer and verifying that customerôs identity using reliable, independent source documents, data or information,
- determining whether the customer is acting on behalf of another person, and then taking reasonable steps to obtain sufficient identification data to verify the identity of that other person,
- identifying the (ultimate) beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the insurer is satisfied that it knows who the beneficial owner is. For legal persons and arrangements insurers should take reasonable measures to understand the ownership and control structure of the customer,
- obtaining information on the purpose and intended nature of the business relationship and other relevant factors,
- conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the insurerôs knowledge of the customer and/or beneficial owner, their business and risk profile, including, where necessary, the source of funds.

8. 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. Subject to national legal requirements insurers may apply reduced or simplified measures in the case of low risk categories.

3 According to the FATF Recommendations beneficial owner 'refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a person or arrangement.

9. 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 for beneficiaries that obviously use fictitious names or whose identity is kept anonymous.

10. Factors to consider when creating a risk profile, which are not set out in any particular order of importance and which should not be considered exhaustive, include (where appropriate):

- type and background of customer and/or beneficial owner,
- the customerôs and/or beneficial ownerôs geographical base,
- the geographical sphere of the activities of the customer and/or beneficial owner,
- the nature of the activities,
- the means of payment as well as the type of payment (cash, wire transfer, other means of payment),
- the source of funds,
- the source of wealth,
- the frequency and scale of activity,
- the type and complexity of the business relationship,
- whether or not payments will be made to third parties,
- whether a business relationship is dormant,
- any bearer arrangements,
- suspicion or knowledge of money laundering, financing of terrorism or other crime.

11. 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 insurer should conduct due diligence at appropriate times. In insurance, various transactions or ótrigger eventsô 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

12. The requirement for an insurer to 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 competent authorities and auditors. In this respect ñtransactionsò 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.

13. 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 insurer should not conclude the insurance contract, perform the transaction, or should terminate the business relationship. The insurer should also consider making a suspicious transaction report (STR) to the financial intelligence unit (FIU).

Establishing a business relationship

14. Before an insurance contract is concluded between customer and insurer there is already a pre-contractual business relationship between these two and possibly other parties. After a policy is taken out:

    - Å the insurer covers a certain risk described in the contract and policy conditions,
    - Å certain transactions may take place such as premium payments, payments of advance or final benefits, and
    - Å certain events may occur such as a change in cover or a change of beneficiaries.

15. The insurer will need to carefully assess the specific background, and other conditions and needs of the customer. This assessment is already being carried out for commercial purposes (determining the risk exposure of the insurer and setting an adequate premium) as well as for reasons of active client management. To achieve this, the insurer will 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.

16. The insurer should realize that creating a customer profile is also of importance for AML/CFT purposes and therefore for the protection of the integrity of the insurer and its business.

17. In addition, the beneficial owner should also be identified and verified. For the purposes of this guidance paper the expression beneficial owner applies to the owner/controller of the policyholder as well as to the beneficiary to the contract.

18. With regard to reinsurance, due to the nature of the business and the lack of a contractual relationship between the policyholder and the reinsurance company, it is often impractical or impossible for the reinsurer to carry out verification of the policyholder or the beneficial owner. Therefore, for reinsurance business reinsurers should only deal with authorized insurers (1) that are licensed or otherwise authorised to issue insurance policies and (2) which have warranted or otherwise confirmed that they apply AML/CFT standards at least equivalent to those in this guidance paper, provided there is no information available to the contrary for instance from FATF and trade associations or from the reinsurersô visits to the premises of the insurer.

19. When the identity of customers and beneficial owners with respect to the insurance contract has been established the insurer 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 (possibly available from industry databases) and on known or suspected terrorists (publicly available on sanctions lists such as those published by the United Nations).

Timing of identification and verification

20. In principle identification and verification of customers and beneficial owners should take place when the business relationship with that person is established. This means that (the owner / controller of) the policyholder needs to be identified and their identity verified before, or at the moment when, the insurance contract is concluded. Valid exceptions are mentioned in the following paragraphs.

21. 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, 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.

22. Where a policyholder and/or beneficiary is permitted to utilise the business relationship prior to verification, financial institutions should be required to adopt risk management procedures concerning the conditions under which this may occur. These procedures should include 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. Where the insurer has already commenced the business relationship and is unable to comply with the verification requirements it should terminate the business relationship and consider making a suspicious transaction report to the FIU.

23. Examples of situations where a business relationship could be used prior to verification are:

- group pension schemes,
- non-face-to-face customers,
- premium payment made before the application has been processed and the risk accepted, and
- using a policy as collateral.

24. In addition, in the case of non-face-to-face business verification may be allowed after establishing the business relationship. However, insurers must have policies and procedures in place to address the specific risks associated with non-face-to-face business relationships and transactions.

Transactions and events in the course of the business relationship

25. The insurer should perform ongoing due diligence on the business relationship. In general the insurer 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. Enhanced due diligence is required with respect to higher risk categories. The Customer Duty Diligence (CDD) program should be established in such a way that the insurer is able to adequately gather and analyse information.

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

- Å a change in beneficiaries (for instance, to include non-family members, or a request for payments to be made to persons other than beneficiaries),
- Å a change/increase of insured capital and/or of the premium payment (for instance, which appear unusual in the light of the policyholderôs income or where there are several overpayments of policy premiums after which the policyholder requests that reimbursement is paid to a third party),
- Å use of cash and/or payment of large single premiums,
- Å payment/surrender by a wire transfer from/to foreign parties,
- Å payment by banking instruments which allow anonymity of the transaction
- Å change of address and/or place of residence of the policyholder, in particular, tax residence,
- Å lump sum top-ups to an existing life insurance contract,
- Å lump sum contributions to personal pension contracts,
- Å requests for prepayment of benefits,
- Å 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),
- Å change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment),
- Å early surrender of the policy or change of the duration (where this causes penalties or loss of tax relief),

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

28. 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. As an example, doubts might arise if benefits from one policy of insurance are used to fund the premium payments of another policy of insurance.

29. The best possible identification documentation should be obtained from each verification subject. ñBest possibleò means that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

Individuals

30. The following personal information should be considered:
- Å full name(s) used,

- Å date and place of birth ,
- Å nationality,
- Å current permanent address including postcode/zip code,
- Å occupation and name of employer (if self-employed, the nature of the self-employment), and
- Å specimen signature of the individual.

31. It is recognised that different jurisdictions have different identification documents. In order to establish identity it is suggested that the following documents may be considered to be the best possible,
    - Å national identity card, or.
    - Å current valid passport

32. Original documents should be signed by the individual and if the individual is met face-to-face, the documents should preferably bear a photograph of the individual. Where copies of documents are provided, appropriate authorities and professionals may certify the authenticity of the copies.

33. Documents which are easily obtained in any name should not be accepted uncritically. These documents include, an identity card issued by the employer of the applicant even if bearing a photograph, credit cards, business cards, provisional driving licences (not bearing a photograph), and student union cards.

Legal persons, companies, partnerships and other institutions/arrangements

34. The types of measures normally needed to perform CDD on legal persons, companies, partnerships and other institutions/arrangements satisfactorily require identification of the natural persons with a controlling interest and the natural persons who comprise the mind and management of the legal person or arrangement. Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to identify and verify the identity of any shareholder of that company.

35. FATF Recommendation 5 requires, where customers and/or beneficial owners are legal persons or legal arrangements, the insurers to:

    - Å verify that any person purporting to act on behalf of the customer and/or beneficial owner is so authorized and identify and verify the identity of that person,
    - Å verify the legal status of the legal person or legal arrangement, e.g. by obtaining proof of incorporation or similar evidence of establishment or existence, and
    - Å form an understanding of the ownership and control structure of the customer and/or beneficial owner.

36. Where trusts or similar arrangements are used, particular care should be taken in understanding the substance and form of the entity. Where the customer is a trust,

the insurer should verify the identity of the trustees, any other person exercising effective control over the trust property, the settlers and the beneficiaries. Should it not be possible to verify the identity of the beneficiaries when the policy is taken out, verification must be carried out prior to any payments being made.

37. When dealing with the identification and verification of companies, trust and other legal entities the insurer should be aware of modes, corporate or otherwise, that are known to be misused for illicit purposes.

38. Sufficient verification should be undertaken to ensure that the individuals purporting to act on behalf of an entity are authorised to do so.

39. The following documents or their equivalent should be considered:

- Å certificate of incorporation,
- Å the name(s) and address(es) of the beneficial owner(s) and/or the person(s) on whose instructions the signatories of the customer are empowered to act,
- Å constitutional documents e.g. memorandum and articles of association, partnership agreements,
- Å copies of powers of attorney or other authorities given by the entity.

40. In all transactions undertaken on behalf of an employer-sponsored pension or savings scheme the insurer should, at a minimum, undertake verification of the principal employer and the trustees of the scheme (if any).

41. Verification of the principal employer should be conducted by the insurer in accordance with the procedures for verification of institutional applicants for business. Verification of any trustees of the scheme will generally consist of an inspection of the relevant documentation, which may include:

- Å the trust deed and/or instrument and any supplementary documentation,
- Å a memorandum of the names and addresses of current trustees (if any),
- Å extracts from public registers,
- Å references from professional advisers or investment managers.

42. As legal controls vary between jurisdictions, particular attention may need to be given to the place of origin of such documentation and the background against which it is produced.

Enhanced measures with respect to higher risk customers and non-cooperative countries and territories

43. 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 customerôs individual risk situation, and the types of business relationships mentioned in the following paragraphs.

44. With regard to enhanced due diligence, in general the insurer should consider which of the following, or possible additional measures, are appropriate:

- Å certification by appropriate authorities and professionals of documents presented requisition of additional documents to complement those which are otherwise required,
- Å 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,
- Å performance of due diligence on source of funds and wealth,
- Å obtaining senior management approval for establishing business relationship,
- Å conducting enhanced ongoing monitoring of the business relationship.

Bearer policies

45. Bearer policies are insurance contract that require the insurer to pay funds to the person(s) holding the policy document or to whom the entitlement to the benefit(s) is endorsed without knowledge or consent of the insurer. This type of policy does not exist in every jurisdiction but, where it does, it could serve as a financial instrument that can easily be exchanged from person to person without the endorsees being identified. Identification and verification by the insurer would only occur at the policyôs maturity when the benefits are being claimed. From the point of view of AML and CFT the use of bearer policies should be discouraged. Where bearer policies are nevertheless permitted in a jurisdiction the insurer should perform appropriate enhanced CDD as specified above.

Viatical arrangements

46. Where a policyholder becomes seriously or terminally ill, he may decide to transfer the entitlement to the benefits of a life insurance policy after his death to a third party in order to receive funds before his death. In some jurisdictions there are ñviaticalò companies that purchase and sell these entitlements. In these cases similar risks exist as described under ñbearer policiesò. Where viatical arrangements are allowed in a jurisdiction, supervisory overview or regulation is recommended. The insurer who needs to pay funds to a viatical company should perform enhanced CDD as specified above including the identification and verification of the viatical company and its beneficial owners.

Politically exposed persons (PEPs)

47. PEPs are defined as individuals who are or have been entrusted with prominent public functions in Sri Lanka or abroad for example Heads of State or of government, senior politician, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not

intended to cover middle ranking or more junior individuals in the foregoing categories.

48. The FATF Recommendations require additional due diligence measures in relation to PEPs. For this purpose insurers should:

- Å have appropriate risk management systems to determine whether the customer is a PEP. 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,
- Å obtain senior management approval for establishing business relationships with such customers,
- Å take reasonable measures to establish the source of wealth and source of funds, and
- Å conduct enhanced ongoing monitoring of the business relationship.

New or developing technologies

49. New or developing technologies can be used to market insurance products. e-commerce or sales through the internet is an example of this. Although for this type of non-face-to-face business verification may be allowed after establishing the business relationship, the insurer should nevertheless complete verification.

50. Although a non-face-to-face customer can produce the same documentation as a face-to-face customer, it is more difficult to verify their identity. Therefore, in accepting business from non-face-to-face customers an insurer should use equally effective identification procedures as those available for face-to-face customer acceptance, supplemented with specific and adequate measures to mitigate the higher risk.

51. Examples of such risk mitigating measures are:

- Å certification by appropriate authorities and professionals of the documents provided,
- Å requisition of additional documents to complement those which are required for face-to-face customers,
- Å independent contact with the customer by the insurer,
- Å third party introduction, e.g. by an intermediary subject to the criteria established in paragraphs,
- Å requiring the first payment to be carried out through an account in the customerôs name with a bank subject to similar CDD standards.

Non-cooperative countries and territories

52. Compliance by jurisdictions with the FATF Recommendations is periodically assessed by international organizations. Jurisdictions that do not sufficiently

apply the FATF Recommendations could be listed by the FATF as Non-Co-operative Countries and Territories (NCCTs). In specific circumstances, jurisdictions may be asked to impose appropriate countermeasures. Insurers should give special attention, especially in underwriting and claims settlement, to business originating from jurisdictions which do not sufficiently apply the FATF Recommendations.

Simplified customer due diligence

53. 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 insurerôs 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 national systems it could be reasonable for insurers to apply, subject to national 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.

54. Insurers should bear in mind that the FATF lists the following examples of customers where simplified or reduced measures could apply:

- Å financial institutions ï where they are subject to requirements to combat money laundering and the financing of terrorism consistent with the FATF Recommendations, and are supervised for compliance with those controls,
- Å public companies that are subject to regulatory disclosure requirements,
- Å government administrations or enterprises.

55. Simplified CDD or reduced measures could also be acceptable for various types of products or transactions.

- Å life insurance policies where the maturity value is less than Rs. 1 million or a single premium of less than Rs.500,000,
- Å insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral,
- Å 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 memberôs interest under the scheme,
- Å general insurance policies where the sum insured is less than Rs. 1 million.

Reliance on intermediaries and third parties

56. Depending on the legislation of the jurisdictions in which the insurer operates, it may be allowed to rely on intermediaries and third parties to perform the following CDD elements:

- identifying the customer and verifying that customerôs identity using reliable, independent source documents, data or information,
- 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 that they know who the beneficial owner is, including taking reasonable measures to understand the ownership and control structure of the customer, and
- obtaining information on the purpose and intended nature of the business relationship.

57. Where such reliance is permitted, the following criteria should be met:

- the insurer should immediately obtain the necessary information concerning the above mentioned elements. Insurers should 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. Insurers should be satisfied with the quality of the due diligence undertaken by the intermediaries and third parties.

- the insurer should satisfy itself that the intermediaries and third parties are regulated and supervised, and have measures in place to comply with CDD requirements in line with FATF Recommendations 5 and 10.

58. Where such reliance is permitted, the ultimate responsibility for customer and/or beneficial owner identification and verification remains with the insurer relying on the intermediaries or third parties. The checks by the insurer 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 insurer should be satisfied that the AML and CFT measures are implemented and operating adequately.

59. Insurers 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 FIU and the insurer in the case of a suspicious transaction. It is recommended that insurers use application forms to be filled out by the customers and/or intermediaries/third parties that include information on identification of the customer and/or beneficial owner as well as the method used to verify their identity.

60. The insurer 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.

Part IV – Anti- Money Laundering Programme

Organization and staff Risk management arrangements

1. Insurers should have in place programmes and systems to prevent money laundering and the financing of terrorism. Each insurerôs programme should be sufficiently robust to effectively and efficiently handle the volume of information processed by that insurer. The programmes and systems should constitute an operational, practical and precise approach for dealing with money laundering and terrorist financing. These programmes and systems should be adapted to the group structure, organisational structure responsibility structure and products and market conditions.

2. These programmes should include the development of internal policies, procedures and controls which, inter alia, should cover:

    - CDD, the detection of unusual or suspicious transactions and the reporting obligation, and the communication of these policies, procedures and controls to the employees,
    - appropriate compliance management arrangements,
    - record keeping arrangements, and
    - adequate screening procedures to ensure high standards when hiring employees
        - an ongoing employee training programme,
        - an adequately resourced and independent audit function to test compliance (e.g. through sample testing) with these policies, procedures, and controls.

3. The development of policies, procedures and controls enables the insurer to comply with legislation and to determine the desired standard of CDD for its own organisation. In order to be able to verify whether the insurer works in compliance with its internal policies, procedures and controls, an audit function should be in place. It is of importance that the audit function is independent and, if applicable, that the auditor has direct access and reports directly to management and the board of directors.

4. It is important that the board of directors and senior management of the insurer establish and support the developed internal policies, procedures and controls and the implementation and adherence thereto. Implementation of internal AML/CFT measures must constitute a relevant priority to insurers. In addition, the board of directors and senior management of an insurer should be kept regularly informed of all significant matters relating to AML/CFT measures and whether the insurer is suspected of being used to launder money or to finance terrorism. This information should be used to evaluate the effectiveness of the programmes and to take appropriate action.

5. Compliance management arrangements should include the appointment of a compliance officer at management level. The compliance officer should be well

versed in the different types of products and transactions which the institution handles and which may give rise to opportunities for money laundering and the financing of terrorism. On receipt of a report from a member of staff concerning a suspicious customer or suspicious transaction the compliance officer should determine whether the information contained in such a report supports the suspicion. The compliance officer should verify the details in order to determine whether the insurer should submit a report to the FIU. The compliance officer should keep a register of all reports to the FIU and a separate register of all reports made to him by staff.

6. Insurers should ensure that:
   - there is a clear procedure for staff to report suspicions of money laundering and the financing of terrorism without delay to the compliance officer,
   - there is a clear procedure for reporting suspicions of money laundering and the financing of terrorism without delay to the FIU, and
   - all staff know to whom their suspicions should be reported.

7. Insurers should ensure that the principles applicable to insurers also apply to branches and majority owned subsidiaries located abroad, 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 supervisor in the jurisdiction of the parent institution should be informed by the insurer that it cannot apply the FATF Recommendations.

8. It is recommended that insurers and other financial institutions should liaise to exchange information on both trends and risks in general and on concrete cases, subject to their obligations concerning privacy and data protection.

Record keeping

9. Insurers should keep records on 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 the account files and business correspondence, for at least six years after the end of the business relationship.

10. Insurers should maintain, for at least six years after the business relationship has ended, all necessary records on transactions, both domestic and international, and be able to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions, including the amount and types of currency involved, if any, so as to provide, if necessary, evidence for prosecution of criminal activity.

11. Insurers 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.

12. **Insurers should ensure that they have adequate procedures**:

- 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 insurers,
- to access all post-sale records associated with the maintenance of the contract, up to and including maturity of the contract, and
- to access details of the maturity processing and/or claim settlement including completed ñdischarge documentationò.

Screening of staff

13. Staff should have the level of competence necessary for performing their duties. Insurers 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.

14. Insurers should identify the key staff within their organisation with respect to AML/CFT and define fit and proper requirements which these key staff should possess. Paragraphs 19 and 20 provide a description of relevant positions.

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

- verification of the identity of the person involved, and
- verification of whether the information and references provided by the employee are correct and complete.

16. 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.

17. Insurers 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.

Training of staff

18. Insurersô staff should receive initial and ongoing training on relevant AML/CFT legislation, regulations, guidance and the insurersô own AML/CFT policies and procedures. Although each insurer should decide for itself how to meet the need to train members of its staff in accordance with its particular legal, regulatory and commercial requirements, the programme will at a minimum include:

- Å a description of the nature and processes of laundering and terrorist financing, including new developments and current money laundering and terrorist financing techniques, methods and trends,
- Å a general explanation of the underlying legal obligations contained in the relevant laws, and
- Å a general explanation of the insurersô AML/CFT policy and systems, including particular emphasis on verification and the recognition of suspicious customers/transactions and the need to report suspicions to the compliance officer.

19. Employees who, due to their assigned work, need more specific training can be divided into two categories.

The first category of employees is those staff who deal with:

- Å new business and the acceptance ï either directly or via intermediaries ï of new policyholders, such as sales persons,
- Å the settlement of claims, and
- Å the collection of premiums or payments of claims.

They need to be made aware of their legal responsibilities and the AML/CFT policies and procedures of the insurer, in particular the client acceptance policies and all other relevant policies and procedures, the requirements of verification and records, the recognition and reporting of suspicious customers/transactions and suspicion of the financing of terrorism. They also need to be aware that suspicions should be reported to the compliance officer in accordance with AML/CFT requirements.

A higher level of instruction covering all aspects of AML/CFT policy and procedure should be provided to the second category of staff, including directors and senior management with the responsibility for supervising or managing staff, and for auditing the system. The training should include:

- Å their responsibility regarding AML/CFT policies and procedures,
- Å relevant laws, including the offences and penalties arising,
- Å procedures relating to the service of production and restraint orders
- Å internal reporting procedures, and
- Å the requirements for verification and record keeping.

20. In addition to the training mentioned in the previous paragraphs, the compliance officer should receive in-depth training concerning all aspects of all relevant legislation and guidance and AML/CFT policies and procedures. The compliance officer will require extensive initial and continuing awareness on the validation and reporting of suspicious customers/transactions, etc.

Part V - Reporting of Suspicious Transactions to the Financial Intelligence Unit

1. If an insurer suspects, or has reasonable grounds to suspect, that funds are the proceeds of a unlawful activity or are related to terrorist financing it should be required to report its suspicions promptly to the FIU.

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

3. Suspicious transactions might fall into one or more of the following examples of categories:
   - Å any unusual financial activity of the customer in the context of his own usual activities,
   - Å any unusual transaction in the course of some usual financial activity
   - Å any unusually linked transactions,
   - Å any unusual or disadvantageous early redemption of an insurance policy,
   - Å 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,
   - Å any unusual method of payment,
   - Å any involvement of any person subject to international sanctions.

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.

5. Insurers, 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 FIU. 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 insurer could then decide not to pursue enhanced due diligence activities but to file a suspicious transaction report.

SUSPICIOUS TRANSACTIONS REPORT (STR) IN TERMS OF FINANCIAL TRANSACTIONS REPORTING ACT NO. 6 OF 2006

Please note that to be accepted as a STR, this form must be completed in all material detail.

a. This report is made pursuant to the requirement to report suspicious transactions under the Financial Transactions Reporting Act No.6 of 2006 (FTRA).
b. Under section 12 of the FTRA, no civil, criminal or disciplinary proceedings shall be brought against a person who makes a report unless it was made in bad faith.

In accordance with Section 7 of the Financial Transactions Reporting Act No. 6 of 2006, the reporting entity is obliged to report suspicious transactions as soon as is practicable after forming that suspicion or receiving the information, but no later than 2 working days to the Financial Intelligence Unit.

Please take note of the following prior to completing the Suspicious Transaction Report (ñSTRò)

- **Provide** a clear and concise description of the STR, and **state** all available information.
- **Document** in detail why the **transaction** is considered extraordinary, irregular or **suspicious.**
- **Provide** supporting documents where it is necessary to explain the STR.
- **Indicate** if the potential violation is an initial report or if it relates to a previous **transaction** or transactions reported.
- **Complete** this STR in Block letters.
- Take reference to the explanatory notes at page 5.

STRICTLY CONFIDENTIAL

Kindly fill in CAPITAL. Read the instructions at page 5 before filling the form.

PART A: DETAILS OF REPORT					
1.1 Date of sending report ☐☐ ☐☐ 2 0 0 ☐ D D M M Y Y Y Y					
1.2 Is this a replacement to an earlier report? ☐No ☐ Yes (Tick ã as applicable)					
1.3 Date of sending original report if this is a replacement report ☐☐☐☐ 2 0 0 ☐ D D M M Y Y Y Y					
PART B: INFORMATION OF POLICY HOLDER					
a)	Policy Holder				
1.	Name in full (if organization, provide registered business/organization name)				
2.	NIC No./ Passport No./Nationality/Business Registration No.				
3.	Gender	Male		Female	
4.	Date of Birth				
5.	Nationality				
6.	Country of Residence				
7.	Business/ Employment Type				
8.	Name of Employer (Where applicable)				
9.	Occupation /profession (where appropriate principal activity of the person conducting transaction)				
10.	Residential/Registered Address				
11.	Name of Father/Mother/Guardian/Spouse				
12.	Telephone No.	☐☐☐☐☐☐☐☐☐☐			
13.	Date of last review of policy holderôs details	☐☐ ☐☐ ☐☐☐☐ D D M M Y Y Y Y			
Brief description of policy holderôs relationship with the insurer.					
b. Details of Policy Contract					
14.	Policy No.	☐☐☐☐☐☐☐☐☐☐☐☐			
15.	Date of Insurance Contract	☐☐ ☐☐ ☐☐☐☐ D D M M Y Y Y Y			
16.	Sum insured				
17.	Name of the Branch				
18.	Business/ Employment Type				
19.	Occupation (Where appropriate, principal activity of the person conducting transaction				
20.	Occupation Description				
21.	Name of Employer (Where applicable)				
22.	Residential/Registered Address				

PART C: DESCRIPTION OF SUSPICIOUS TRANSACTION		
23.	Ground for suspicion (Please mark ã where relevant)	
	☐ Customer insisting on anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information; ☐ A change in beneficiaries (for instance, to include non-family members, or a request for payments to be made to personôs other than beneficiaries); ☐ A change/increase of insured capital and/or of the premium payment (for instance, which appear unusual in the light of the policyholderôs income or where there are several overpayments of policy premiums after which the policy holder requests that reimbursement is paid to a third party); ☐ Use of cash and /or payment of large single premiums; ☐ Payment/surrender by a wire transfer from/to foreign parties; ☐ Payments by banking instruments which allow anonymity of the transaction change of address and/or place of residence of the policyholder; ☐ Lump sum top-ups to an existing life insurance contract; ☐ Lump sum contributions to personal pension contracts; ☐ Requests for prepayment of benefits; ☐ 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) ☐ Change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment. ☐ Early surrender of the policy or change of the duration (where this causes penalties or loss of tax relief); ☐ Frequent request for changing address ☐ Any other reasons please specify	
24. Provide details of nature and the circumstances: (Could be included as additional attachments)		

]

PART D: DETAILS OF REPORTING OFFICER & COMPLIANCE OFFICER

25. Date of Reporting: ☐☐ ☐☐ 2 0 0 ☐

D D M M YY Y Y

Reporting Officer: é ..... é é é é é é

Designation:é é é é é é é é é é é é ..

Name of Compliance Officer

Address: é é é é é é é é é é é é é é

Contact No. é é é é é é é é é .. E-mailé é é é é é é . Fax é é é é ..

é é é é é é é é é é é é é .

Signature of Compliance Officer

PART E: FOR FIU OF SRI LANKA USE ONLY

Receiving Officer

Date Received: ☐☐ ☐☐ 2 0 0 ☐

D D M M Y Y Y Y

STR No: ☐☐☐☐☐☐☐☐☐☐

Date of Acknowledgement: ☐☐ ☐☐ 2 0 0 ☐

D D M M Y Y Y Y

FIU ACKNOWLEDGEMENT

Received by the Financial Intelligence Unit of the Central Bank , STR No. ☐☐☐☐☐☐☐☐☐

dated ☐☐ ☐☐ 200 ☐

fromé é é é é é é é é

é é é é é é é é é é é é é é é é .

Director/FIU

SUSPICIOUS TRANSACTION REPORT (STR) IN TERMS OF FINANCIAL TRANSACTIONS REPORTING ACT NO. 6 OF 2006 INSTRUCTIONS

GENERAL INSTRUCTIONS

Under the **FINANCIAL TRANSACTIONS REPORTING ACT, NO. 6 OF 2006 (FTRA)**, every reporting institution shall furnish details of suspicious transactions defined in Section 7 (1) of the FTRA Act .

7 (1) Where an Institution -

(a) has reasonable grounds to suspect that any transaction or attempted transaction may be related to the commission of any unlawful activity or any other criminal offence; or

(b) has information that it suspects may be relevant ---

(i) to an act preparatory to an offence under the provision of the Convention on the Suppression of Financing of Terrorism Act, No. of 2005.

(ii) to an investigation or prosecution of a person or persons for an act constituting an unlawful activity, or may otherwise be of assistance in the enforcement of the Money laundering Act. No.5 of 2006 and the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005.

How to submit

Every institution must submit this form to the Director, FIU only through the Compliance Officer of the reporting institution designated under the FTRA. In urgent cases, the form should also be sent by fax:

Address: Director
Financial Intelligence Unit
Central Bank of Sri Lanka
30, Janadhipathi Mawatha
Colombo 1.
Fax. 94 11 2477692

EXPLANATION OF SPECIFIC TERMS

PART A: DETAILS OF REPORT

1.1 Date of sending report is the date on which the compliance officer sends the report to Director (FIU).

1.2 and 1.3

Replacement report is a report submitted in replacement of an earlier STR. When a replacement report is submitted, date of submitting original STR may be mentioned and the complete STR has to be submitted again.

PART B Information of Policy Holder

PART C: Description Of Suspicious Transaction

PART D: DETAILS OF REPORTING OFFICER/ COMPLIANCE OFFICER Compliance officer is the officer designated by the reporting institution under the FTRA.

ALL ANNEXURES MUST BE ENCLOSED

*