Guidance Paper No. 5

INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

GUIDANCE PAPER ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

OCTOBER 2004

This document was prepared by the Insurance Fraud Subcommittee,
in consultation with members and observers

It replaces the *Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities* (January 2002)

Guidance paper on anti-money laundering and combating the financing of terrorism

Contents

1. Introduction

1. The insurance sector[1] and 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 organising 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.

2. Although its vulnerability is not regarded by the International Association of Insurance Supervisors (IAIS[2]) to be as high as for other sectors of the financial industry, the insurance sector is a possible target for money launderers and for those seeking resources for terrorist acts or for ways to process funds to accomplices. Insurers can be involved, knowingly or unknowingly, in money laundering and the financing of terrorism. This exposes them to legal, operational and reputational risks.[3] The insurance sector should therefore take adequate measures to prevent its misuse by money launderers and terrorists, and should address possible cases of money laundering and terrorist financing forthwith.

3. The IAIS has given anti-money laundering (AML) and combating the financing of terrorism (CFT) high priority. In October 2003 the IAIS approved and issued the *Insurance core principles and methodology*, which revised the core principles for the supervision of

1 The insurance sector includes insurers, reinsurance companies and intermediaries. The word "intermediaries" shall, in the context of this paper, mean agents, brokers and any other form of mediation or delegation of authority on behalf of an insurer.

2 All abbreviated terms are defined in the list of abbreviations in Appendix D.

3 Legal risk: the possibility that lawsuits, adverse judgements or contracts that turn out to be unenforceable disrupt or adversely affect the operations or condition of an insurer. Reputational risk: the potential that adverse publicity regarding an insurer´s business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Operational risk: the risk arising from failure of systems, internal procedures and controls leading to financial loss. Operational risk also includes custody risk.

insurers. Compliance with the Insurance Core Principles is required for a supervisory system to be effective. In accordance with Insurance Core Principle 28 (see appendix B) the Recommendations of the Financial Action Task Force on Money Laundering (FATF) applicable to the insurance sector and to insurance supervision must be satisfied to reach this objective.

4. In June 2003 the FATF adopted a revised set of Forty Recommendations on AML/CFT, having adopted VIII Special Recommendations on Terrorist Financing to combat the financing of terrorism[4] in October 2001.

5. The IAIS considers the FATF Forty Recommendations 2003 on Money Laundering and the FATF VIII Special Recommendations on Terrorist Financing to be the international standards in the field of AML/CFT for insurance supervisors and the insurance sector.
According to FATF Recommendation 25 the "competent authorities [of each jurisdiction] should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions".

6. In light of the FATF Recommendations, the IAIS considers there is need for specific guidance for insurance supervisors and the insurance sector. This guidance paper is intended to provide such guidance and aims at tailoring the existing AML/CFT standards to the specific practices and features of the insurance sector.

7. The FATF Recommendations are applicable to the underwriting and placement of life insurance and other investment related insurance. This paper applies at a minimum to those insurers and intermediaries offering life insurance products or other investment related insurance.

8. The IAIS is concerned to ensure that the potential risks to types of insurance other than life insurance (non-life insurance and reinsurance) are also considered by insurance supervisors and insurers. Jurisdictions or the supervisor could decide to extend AML/CFT policies and guidance beyond the scope of the FATF Recommendations on the basis of a thorough analysis of the risk of money laundering or financing of terrorism for these other types of insurance. In the case of such a decision the regulator and/or supervisor concerned should determine the appropriate policies and guidance as described in this paper to adequately cover the risks involved. This does not imply that the full set of measures presented in this paper should be implemented in these cases. Where a jurisdiction/supervisor chooses to expand its AML/CFT policies and regulation to include non-life insurance and/or reinsurance, this paper offers a range of measures and procedures from which the jurisdiction/supervisor can determine the most effective. The type and extent of these policies and guidance imposed should be appropriate, having regard to these risks and the size of the business.

9. The same principles that apply to insurers should generally apply to insurance intermediaries.

10. Each insurance supervisor should consider whether to issue this guidance paper and/or its own guidance, at least equivalent to the standards in this paper, to insurers in its own jurisdiction. Each supervisor is responsible for issuing appropriate AML/CFT guidance.

4 These recommendations can be found on the FATF website (www.fatf-gafi.org). FATF Recommendations 4-6, 8-11, 13-15, 17, 21-23, 25, 29-32 and 40 as well as Special Recommendations IV, V, VII and the AML/CFT Methodology are specifically of importance for insurers and insurance supervisors.

11. This guidance paper is structured as follows:

- Sections 2 and 3 constitute a risk-based approach regarding the combating of money laundering and the financing of terrorism in the insurance sector.
- Section 2 explains the risk of money laundering and the financing of terrorism starting with a general description of the process of money laundering and the financing of terrorism and then explaining in more detail how this could be effected through the various types of insurance.
- Section 3 presents a set of measures and procedures to control the risks described in section 2. Section 3 discusses in more detail:
  - elements of customer due diligence (CDD)
  - reporting of suspicion
  - measures affecting the organisation and staff of the insurer.
- Section 4 is addressed to supervisors and deals with their application of the Insurance Core Principles, including the monitoring of compliance by insurers with AML/CFT standards and cooperation by supervisors with other organisations involved in AML/CFT. This section is specifically addressed to supervisors.

2. Money laundering and financing of terrorism in insurance

The process of money laundering and financing of terrorism

12. Money laundering is the processing of the proceeds of crime to disguise their illegal origin. Once these proceeds are successfully 'laundered' the criminal is able to enjoy these monies without revealing their original source. Money laundering can take place in various ways. Information on possible trends and techniques used by money launderers is collected by the FATF in the course of its annual typology exercise.[5]

13. Financing of terrorism can be defined as the wilful 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

14. 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.

15. 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 More information on typologies can be found on the website of the FATF (www.fatf-gafi.org).

- (second hand) endowment policies.

16. 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.

17. 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 insurer's 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 worker's compensation payments to support terrorists awaiting assignment and primary coverage and trade credit for the transport of terrorist materials. This could also imply breach of regulations requiring the freezing of assets.

18. 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.

19. 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.[6]

20. Specific cases and examples of money laundering involving insurance are included in more detail in appendix C to this paper.

6 See FATF Recommendation 9

3. Control measures and procedures against money laundering and financing of terrorism

21. This section is structured as follows. After an introduction of the duty of vigilance:

- paragraphs 25-83 contain a description of the customer due diligence process
- paragraphs 84-88 describe measures and procedures for the reporting of suspicious transactions, and
- paragraphs 89-112 provide the arrangements that need to be made to the organisation of the insurer with respect to risk management, record keeping, screening and the training of staff.

The paragraphs on customer due diligence provide measures and procedures on:

- CDD in general and the link with the overall and client[7] acceptance policies of the insurer
- CDD when establishing a business relationship
- timing of identification and verification
- CDD in the course of the business relationship
- the methods of identification for individuals and for companies, partnerships and other institutions/arrangements
- enhanced CDD for higher risk customers and non-cooperative countries and territories (NCCTs) (including bearer policies, viatical arrangements, politically exposed persons (PEP) and new technologies)
- simplified CDD, and
- reliance on intermediaries and third parties.

22. 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.

23. For reasons of sound business practice and proper risk management insurers should already have controls in place to assess the risk of each business relationships. As customer due diligence is a business practice suitable not just for commercial risk assessment and fraud prevention[8] 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 – it extends to identification of the potential risks of the whole business relationship.

24. 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 organisation and the staff of the insurer, such as a compliance and audit environment, keeping of records, the recruitment of staff and training.

7 The term “client” in this paper refers to customers and beneficial owner unless a different meaning follows from the wording or context of the paragraphs involved.

8 See ICP 27 on Fraud

Performing due diligence on customers, beneficial owners and beneficiaries

25. Insurers should know the customers[9] 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.

26. The insurer's strategic policies will determine its exposure to risks such as underwriting risk, reputational risk, operational risk, concentration risk[10] and legal risk. After determining the strategic policies, client acceptance policies should be established, taking account of risk factors such as the background and geographical base of the customer and/or beneficial owner[11] and the complexity of the business relationship (see paragraph 31 for other factors). 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.

27. 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.

28. Customer due diligence measures that should be taken by insurers include:[12]

- identifying the customer and verifying that customer's 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 insurer's knowledge of the customer and/or beneficial owner, their business and risk profile, including, where necessary, the source of funds.

---

9 Under normal conditions the term 'customer' refers to 'policyholder'.

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

11 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 legal person or arrangement." For the purposes of this paper the expression 'beneficial owner' applies to the owner/controller of the policyholder as well as to the beneficiary to the contract.

12 FATF Recommendation 5

29. 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.

30. 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.

31. 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 customer's and/or beneficial owner's 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.

32. 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.[13] In insurance, various transactions or 'trigger events' 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 (see also paragraph 47).

33. 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.[14] In this respect "transactions" should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, premium payments, requests for changes in benefits, beneficiaries, duration, etc.

13 FATF Recommendation 5

14 FATF Recommendation 11

34. 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).[15]

Establishing a business relationship

35. 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:

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

36. 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.

37. The insurer should realise 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.

38. 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.

39. 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 ceding 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 reinsurers' visits to the premises of the insurer.

40. 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). The IAIS recommends that insurers use available sources of information when considering whether or not to accept a risk. Identification and subsequent

15 See paragraphs 84-88

verification will also prevent anonymity of policyholders or beneficiaries and the use of fictitious names.[16]

Timing of identification and verification

41. In principle identification and verification of customers and beneficial owners should take place when the business relationship with that person is established.[17] 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 contact is concluded. Valid exceptions are mentioned in the following paragraphs.

42. 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.[18]

43. 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.

44. 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.

45. 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[19] (see paragraphs 71-73).

Transactions and events in the course of the business relationship

46. 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

16 FATF Recommendation 5

17 FATF Recommendation 5

18 Interpretative Note no 6 to FATF Recommendation 5

19 FATF Recommendation 8

categories. The CDD program should be established in such a way that the insurer is able to adequately gather and analyse information.

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

- a change in beneficiaries (for instance, to include non-family members, or a request for payments to be made to persons 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 policyholder's income or where there are several overpayments of policy premiums after which the policyholder 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
- payment by banking instruments which allow anonymity of the transaction
- change of address and/or place of residence of the policyholder, in particular, tax residence
- 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)
- request for payment of benefits at the maturity date.

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

49. 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.[20] 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.

Methods of identification and verification

50. This guidance paper does not seek to specify what, in any particular case, may or may not be sufficient evidence to complete verification. It does set out what, as a matter of good practice, may reasonably be expected of insurers. Since, however, this guidance paper is neither mandatory nor exhaustive, there may be cases where an insurer has properly satisfied itself that verification has been achieved by other means which it can justify to the appropriate authorities as reasonable in the circumstances.

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

20 Interpretative Note no 5 to FATF Recommendation 5

Individuals

52. The following personal information should be considered:

- full name(s) used
- date and place of birth
- nationality
- current permanent address including postcode/zipcode[21]
- occupation and name of employer (if self-employed, the nature of the self-employment), and
- specimen signature of the individual.

53. 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, in descending order of acceptability:

- current valid passport; or
- national identity card.

54. However, some jurisdictions do not have national identity cards and many individuals do not possess passports. Where appropriate the jurisdictions or insurance supervisors should compile their own list in accordance with local conditions.

55. 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.

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

Legal persons, companies, partnerships and other institutions/arrangements

57. 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.

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

- verify that any person purporting to act on behalf of the customer and/or beneficial owner is so authorised and identify and verify the identity of that person
- 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
- form an understanding of the ownership and control structure of the customer and/or beneficial owner.

21 In this context "current permanent address" means the verification subject's actual residential address, as it is an essential part of identity.

59. 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 settlors 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.

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

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

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

- certificate of incorporation
- 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
- constitutional documents e.g. memorandum and articles of association, partnership agreements
- copies of powers of attorney or other authorities given by the entity.

63. 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).

64. 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:

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

65. 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

66. Enhanced CDD measures should apply to all higher risk business relationships, clients and transactions. This includes both high risk business relationships assessed by the insurer, based on the customer's individual risk situation, and the types of business relationships mentioned in the following paragraphs.

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

- certification by appropriate authorities and professionals of documents presented

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

Bearer policies

68. 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 policy's 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

69. 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 "viatical" companies that purchase and sell these entitlements. In these cases similar risks exist as described under "bearer policies". 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[22]

70. The FATF Recommendations require additional due diligence measures in relation to PEPs.[23] For this purpose insurers should:

- 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.
- obtain senior management approval for establishing business relationships with such customers
- take reasonable measures to establish the source of wealth and source of funds, and
- conduct enhanced ongoing monitoring of the business relationship.

New or developing technologies

71. 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-

22 According to the FATF Recommendations Politically Exposed Persons (PEPs) are "individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, 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."

23 FATF Recommendation 6

face-to-face business verification may be allowed after establishing the business relationship, the insurer should nevertheless complete verification.

72. 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.

73. Examples of such risk mitigating measures are:

- certification by appropriate authorities and professionals of the documents provided
- requisition of additional documents to complement those which are required for face-to-face customers
- independent contact with the customer by the insurer
- third party introduction, e.g. by an intermediary subject to the criteria established in paragraphs 78-83
- requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Non-cooperative countries and territories

74. Compliance by jurisdictions with the FATF Recommendations is periodically assessed by international bodies.[24] Jurisdictions that do not sufficiently apply the FATF Recommendations could be listed by the FATF as NCCTs. In specific circumstances, jurisdictions may be asked to impose appropriate countermeasures.[25] 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

75. 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 insurer's own assessment), and if information on the identity of the customer and the beneficial owner is publicly available, or adequate checks and controls exist elsewhere in 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[26] and other parties to the business relationship.

76. Insurers should bear in mind that the FATF lists the following examples of customers where simplified or reduced measures could apply:[27]

- financial institutions – 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
- public companies that are subject to regulatory disclosure requirements
- government administrations or enterprises.[28]

---

24 Mutual evaluations under the aegis of the FATF or the Financial Sector Assessment Program by IMF / World Bank.

25 FATF Recommendation 21

26 Interpretative Note no 9 to FATF Recommendation 5

27 Jurisdictions and/or supervisors should assess from an AML and CFT perspective whether the specific circumstances in their insurance sector allow for the simplified or reduced CDD measures, as presented in this and the following paragraph, to be applied.

28 Interpretative Note no 10 to FATF Recommendation 5

77. Furthermore, the FATF states that simplified CDD or reduced measures could also be acceptable for various types of products or transactions such as (examples only):

- life insurance policies where the annual premium is no more than USD/€ 1000 or a single premium of no more than USD/€ 2500
- insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral
- 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.[29]

Reliance on intermediaries and third parties[30]

78. 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:[31]

- identifying the customer and verifying that customer's 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.

79. 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.

80. 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.

81. 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

29 Interpretative Note no 12 to FATF Recommendation 5

30 The following paragraphs 78-83 do not apply to outsourcing or agency relationships other than relationships with insurance agents and brokers.

31 FATF Recommendation 9

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.

82. Each jurisdiction should determine in which jurisdictions the intermediaries and third parties that meet the conditions can be based. Insurers should inform themselves as to which jurisdictions are considered suitable taking into account information available on whether those jurisdictions adequately apply the FATF Recommendations.[32]

83. 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.

Reporting of suspicious transactions to the Financial Intelligence Unit[33]

84. If an insurer suspects, or has reasonable grounds to suspect, that funds are the proceeds of a criminal activity or are related to terrorist financing it should be required to report its suspicions promptly to the FIU.[34] [35] [36]

85. 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.

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

- any unusual financial activity of the customer in the context of his own usual activities
- any unusual transaction in the course of some usual financial activity
- any unusually linked transactions
- any unusual or disadvantageous early redemption of an insurance policy
- 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
- any unusual method of payment
- any involvement of any person subject to international sanctions.

87. 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.

---

32 See FATF Recommendation 9, last sentence. NCCTs should not be considered to be suitable jurisdictions.

33 In this paper "suspicious transaction" includes suspicious activities.

34 FATF Recommendation 13

35 Pursuant to FATF Recommendation 26 countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of suspicious transaction reports (STR) and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

36 According to FATF Recommendation 14 insurers, their directors, officers and employees should be protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

88. 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.[37] 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 these due diligence activities but to file a suspicious transaction report.

Organisation and staff

Risk management arrangements

89. Insurers should have in place programmes and systems to prevent money laundering and the financing of terrorism. Each insurer's 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 (e.g. joint back office), responsibility structure and products and market conditions.

90. 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, e.g. at a minimum the designation of an AML/CFT compliance officer
  - 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.[38]

91. 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.

92. 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.

37 FATF Recommendation 14

38 FATF Recommendation 15 and *Methodology for assessing compliance with anti-money laundering and combating the financing of terrorism standards* 2004

93. Compliance management arrangements should include the appointment of a compliance officer[39] at management level.[40] 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.[41]

94. 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.

95. 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.[42]

96. 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. The IAIS encourages trade associations to promote and/or facilitate this exchange of information.

Record keeping

97. 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 five years after the end of the business relationship.[43] For insurers this implies that there are prescribed periods for keeping relevant records for at least five years after the expiry of policies.

98. Insurers should maintain, for at least five 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

39 The term ‚compliance officer' may in some jurisdictions be referred to as the money laundering reporting officer.

40 Interpretative notes to FATF Recommendation 15

41 Including agency and temporary staff.

42 FATF Recommendation 22

43 FATF Recommendation 10

types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.[44]

99. 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.

100. 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 "discharge documentation".

101. Records should be available to domestic competent authorities upon appropriate authority.[45]

Screening of staff [46]

102. 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.

103. 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 109, 111 and 112 provide a description of relevant positions.

104. The responsibility for initial and on-going assessment of the fitness and propriety of staff lies with the insurer.[47] The procedures concerning the assessment of whether staff meet 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.

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

106. 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.

---

44 FATF Recommendation 10

45 FATF Recommendation 10

46 This section deals with the assessment of staff other than directors and managers that are subject to fit and proper tesing pursuant to Insurance Core Principle 7 ("Suitability of persons") and the IAIS *Guidance paper on fit and proper principles and their application*.

47 Insurance Core Principle 7

Training of staff

107. Insurers' staff should receive initial and ongoing training on relevant AML/CFT legislation, regulations, guidance and the insurers' 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:

- 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
- a general explanation of the underlying legal obligations contained in the relevant laws, and
- a general explanation of the insurers' 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.

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

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

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

110. 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 systems.

111. 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:

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

112. 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 instruction on the validation and reporting of suspicious customers/transactions and freezing assets in accordance with legislation.

4. Role of the supervisor

113. Supervisory authorities, in conjunction with law enforcement authorities and in cooperation with other supervisors, must adequately supervise insurers for AML/CFT purposes in order to assess their ability to prevent and counter such threats.

Application of relevant insurance core principles

114. According to the IAIS Insurance Core Principles a sound regulatory and supervisory system is necessary for maintaining efficient, safe, fair and stable insurance markets. The 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.

115. 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[48]); and the internal control measures of the insurers are relevant in this context.

116. 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.

117. 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.

118. 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.[49]

119. 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 (see paragraphs 126, 127 and 128).

120. The supervisor should be provided with adequate financial, human and technical resources to prevent or assess the insurance sector's 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

48 In accordance with ICP 7 ("Suitability of persons") and the IAIS *Guidance paper on fit and proper principles and their application*.

49 FATF Recommendation 29

legislation, money laundering and terrorist financing typologies and techniques used to monitor compliance with AML/CFT standards by insurers.[50]

Monitoring compliance

121. 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.

122. When conducting on-site inspections the supervisor should consider the insurer's 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 STRs to the FIU.

123. 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

124. 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.

125. 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.

126. The IAIS encourages the supervisor to take all necessary steps to cooperate with the other relevant authorities.

127. It is recommended that the supervisor appoints within its office a contact for AML/CFT issues and to liaise with other national authorities to promote an efficient exchange of information on both trends and risks in general, policy issues and on concrete cases. Contact with the national FIU and law enforcement agencies is recommended to highlight issues of compliance by insurers and to obtain feedback on reported cases.

128. At an international level these contacts could liaise with fellow insurance supervisors to share information on trends and typologies and to deal with incidents with an international dimension.

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

50 FATF Recommendation 30

- 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
- countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide cooperation
- the competent authorities, including the supervisor, should be able to conduct inquiries and, where possible, investigations on behalf of foreign counterparts.

130. 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.[51]

131. 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, memoranda of understanding, exchanges on the basis of reciprocity, or liaison through appropriate international or regional organisations.[52]

51 FATF Recommendation 40

52 Interpretative notes to Recommendation 40

Appendix A – References

References

- Financial Action Task Force (FATF), *Special Recommendations on Terrorist Financing*, October 2001

- FATF, *Report on Money Laundering Typologies*, 2002-2003

- FATF, *The Forty Recommendations*, June 2003

- FATF, *Report on Money Laundering and Terrorist Financing Typologies*, 2003-2004

- FATF, *Methodology for Assessing Compliance with the FATF 40 Recommendations and the 8 Special Recommendations*, February 2004

- International Association of Insurance Supervisors (IAIS), *Insurance Core Principles and Methodology*, October 2003

- IAIS, *Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities*, January 2002

Appendix B – IAIS Insurance Core Principle on AML/CFT

ICP 28 Anti-money laundering, combating the financing of terrorism (AML/CFT)

The supervisory authority requires insurers and intermediaries, at a minimum those insurers and intermediaries offering life insurance products or other investment related insurance, to take effective measures to deter, detect and report money laundering and the financing of terrorism consistent with the Recommendations of the Financial Action Task Force on Money Laundering (FATF).

Explanatory note

28.1. In most IAIS member jurisdictions, money laundering and financing of terrorism are criminal acts under the law. Money laundering is the processing of criminal proceeds to disguise their illegal origin. The financing of terrorism involves the direct or indirect provision of funds, whether lawfully or unlawfully obtained, for terrorist acts or to terrorist organisations.

28.2. Insurers and intermediaries, in particular those insurers and intermediaries offering life insurance or other investment related insurance could be involved, knowingly or unknowingly, in money laundering and financing of terrorism. This exposes them to legal, operational and reputational risks. Supervisory authorities, in conjunction with law enforcement authorities and in co-operation with other supervisors, must adequately supervise insurers and intermediaries for AML/CFT purposes to prevent and counter such activities.

Essential criteria

a. The measures required under the AML/CFT legislation and the activities of the supervisors should meet the criteria under those FATF Recommendations applicable to the insurance sector.[53]

b. The supervisory authority has adequate powers of supervision, enforcement and sanction in order to monitor and ensure compliance with AML/CFT requirements. Furthermore, the supervisory authority has the authority to take the necessary supervisory measures to 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 or an intermediary.

c. The supervisory authority has appropriate authority to co-operate effectively with the domestic Financial Intelligence Unit (FIU) and domestic enforcement authorities, as well as with other supervisors both domestic and foreign, for AML/CFT purposes.

d. The supervisory authority devotes adequate resources – financial, human and technical – to AML/CFT supervisory activities.

e. The supervisory authority requires insurers and intermediaries, at a minimum those insurers and intermediaries offering life insurance products or other investment related

53 See FATF Recommendations 4-6, 8-11, 13-15, 17, 21-23, 25, 29-32 and 40 as well as Special Recommendations IV, V and the AML/CFT Methodology for a description of the complete set of AML/CFT measures that are required.

insurance, to comply with AML/CFT requirements, which are consistent with the FATF Recommendations applicable to the insurance sector, including:

- performing the necessary customer due diligence (CDD) on customers, beneficial owners and beneficiaries
- taking enhanced measures with respect to higher risk customers
- maintaining full business and transaction records, including CDD data, for at least 5 years
- monitoring for complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose
- reporting suspicious transactions to the FIU
- developing internal programmes (including training), procedures, controls and audit functions to combat money laundering and terrorist financing
- ensuring that their foreign branches and subsidiaries observe appropriate AML/CFT measures consistent with the home jurisdiction requirements.

Appendix C – Specific cases and examples of money laundering involving insurance

This appendix contains examples of money laundering or suspicious transactions involving insurance. It will be published on the IAIS website (www.iaisweb.org) as a separate document and updated whenever new examples involving insurance are reported.

Indicators

The following examples may be indicators of a suspicious transaction and give rise to a suspicious transaction report:

- 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) = 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.

The above indicators are not exhaustive.

Life insurance

- A company director from Company W, Mr. H, set up a money laundering scheme involving two companies, each one established under two different legal systems. Both of the entities were to provide financial services and providing financial guarantees for which he would act as director. These companies wired the sum of USD 1.1 million to the accounts of Mr. H in Country S. It is likely that the funds originated in some sort of criminal activity and had already been introduced in some way into the financial system. Mr. H also received transfers from Country C. Funds were transferred from one account to another (several types of accounts were involved, including both current and savings accounts). Through one of these transfers, the funds were transferred to Country U from a current account in order to make payments on life insurance policies. The investment in these policies was the main mechanism in the scheme for laundering the funds. The premiums paid for the life insurance policies in Country U amounted to some USD 1.2 million and represented the last step in the laundering operation.[54]

- An attempt was made to purchase life policies for a number of foreign nationals. The underwriter was requested to provide life coverage with an indemnity value identical to the premium. There were also indications that in the event that the policies were to be cancelled, the return premiums were to be paid into a bank account in a different jurisdiction to the assured.

- On a smaller scale, local police authorities were investigating the placement of cash by a drug trafficker. The funds were deposited into several bank *accounts* and then transferred to an *account* in another jurisdiction. The drug trafficker then entered into a USD 75,000 life insurance policy. Payment for the policy was made by two separate wire transfers from the overseas *accounts*. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker's arrest, the insurer had received instructions for the early surrender of the policy.

54 FATF Report on Money Laundering Typologies, 2002 – 2003

- In 1990, a British insurance sales agent was convicted of violating a money laundering statute. The insurance agent was involved in a money laundering scheme in which over USD 1.5 million was initially placed with a bank in England. The "layering process" involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent's supervisor was also charged with violating the money laundering statute.

  This case has shown how money laundering, coupled with a corrupt employee, can expose an insurance company to negative publicity and possible criminal liability.

- Customs officials in Country X initiated an investigation which identified a narcotics trafficking organisation utilised the insurance sector to launder proceeds. Investigative efforts by law enforcement agencies in several different countries identified narcotic traffickers were laundering funds through Insurance firm Z located in an off-shore jurisdiction.

  Insurance firm Z offers investment products similar to mutual funds. The rate of return is tied to the major world stock market indices so the insurance policies were able to perform as investments. The account holders would over-fund the policy, moving monies into and out of the fund for the cost of the penalty for early withdrawal. The funds would then emerge as a wire transfer or cheque from an insurance company and the funds were apparently clean. To date, this investigation has identified that over USD 29 million was laundered through this scheme, of which over USD 9 million dollars has been seized. Additionally, based on joint investigative efforts by Country Y (the source country of the narcotics) and Country Z customs officials, several search warrants and arrest warrants were executed relating to money laundering activities involved individuals associated with Insurance firm Z.[55]

- A customer contracted life insurance of a 10 year duration with a cash payment equivalent to around USD 400,000. Following payment, the customer refused to disclose the origin of the funds. The insurer reported the case. It appears that prosecution had been initiated in respect of the individual's fraudulent management activity.

- A life insurer learned from the media that a foreigner, with whom it had two life-insurance contracts, was involved in Mafia activities in his/her country. The contracts were of 33 years duration. One provided for a payment of close to the equivalent of USD 1 million in case of death. The other was a mixed insurance with value of over half this amount.

- A client domiciled in a country party to a treaty on the freedom of cross-border provision of insurance services, contracted with a life insurer for a foreign life insurance for 5 years with death cover for a down payment equivalent to around USD 7 million. The beneficiary was altered twice: 3 months after the establishment of the policy and 2 months before the expiry of the insurance. The insured remained the same. The insurer reported the case. The last beneficiary - an alias - turned out to be a PEP.

55 FATF Report on Money Laundering and Terrorist Financing Typologies, 2003 – 2004

Non-life insurance

- A money launderer purchased marine property and casualty insurance for a phantom ocean-going vessel. He paid large premiums on the policy and suborned the intermediaries so that regular claims were made and paid. However, he was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy. In this way, the money launderer was able to receive claims cheques which could be used to launder funds. The funds appeared to come from a reputable insurance company, and few questioned the source of the funds having seen the name of the company on the cheque or wire transfer. [56]

- Four broking agencies were forced to freeze funds after US court action that followed an investigation into Latin American drugs smuggling. The drug trafficking investigation, codenamed Golden Jet, was coordinated by the Drug Enforcement Agency (DEA) based in the USA but also involved the FBI and the UK authorities. The funds frozen by the court action related to insurance money deposited at insurance brokers for around 50 aircraft.

  It is understood that the brokers affected by the court order included some of the largest UK insurance brokers. The case highlighted the potential vulnerability of the insurance market to sophisticated and large scale drug trafficking and money laundering operators. The court order froze aircraft insurance premiums taken out by 17 Colombian and Panamanian air cargo companies and by 9 individuals. The action named 50 aircraft, including 13 Boeing 727s, 1 Boeing 707, 1 French Caravelle and 2 Hercules C130 transport aircraft. The British end of the action was just one small part of a massive anti-drug trafficking action co-ordinated by the DEA. Officials of the DEA believe Golden Jet is one of the biggest blows they have been able to strike against the narcotics trade. The American authorities led by the DEA swooped on an alleged Colombian drugs baron and tons of cocaine valued at many billions of dollars were seized and a massive cocaine processing factory located in Colombia together with aircraft valued at more than USD22 million were destroyed in the DEA coordinated action. According to the indictment, the cargo companies were responsible for shipping tons of cocaine from South to North America all through the 1980s and early 1990s, providing a link between the producers and the consumers of the drugs. Much of the cocaine flowing into the USA was transported into the country by air. During this period the Colombian cartels rose to wealth and prominence, aided by those transport links.

Intermediaries

- A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of USD 250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raise no suspicion at the bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling USD 250,000, thus avoiding the raising suspicions with the insurance company.[57]

56 FATF Report on Money Laundering and Terrorist Financing Typologies, 2003 – 2004

57 FATF Report on Money Laundering Typologies, 2002 – 2003

- Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks. The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses but coming away with a clean cheque from the institution. On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.[58]

- An insurance company was established by a well-established insurance management operation. One of the clients, a Russian insurance company, had been introduced through the management of the company's London office via an intermediary. In this particular deal, the client would receive a "profit commission" if the claims for the period were less than the premiums received. Following an on-site inspection of the company by the insurance regulators, it became apparent that the payment route out for the profit commission did not match the flow of funds into the insurance company's account. Also, the regulators were unable to ascertain the origin and route of the funds as the intermediary involved refused to supply this information. Following further investigation, it was noted that there were several companies involved in the payment of funds and it was difficult to ascertain how these companies were connected with the original insured, the Russian insurance company.

- A construction project was being financed in Europe. The financing also provided for a consulting company's fees. To secure the payment of the fees, an investment account was established and a sum equivalent to around USD 400,000 deposited with a life-insurer. The consulting company obtained powers of attorney for the account. Immediately following the setting up of the account, the consulting company withdrew the entire fee stipulated by the consulting contract. The insurer reported the transaction as suspicious. It turns out that an employee of the consulting company was involved in several similar cases. The account is frozen.

Reinsurance

- An insurer in country A sought reinsurance with a reputable reinsurance company in country B for its directors and officer cover of an investment firm in country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer which contacted law enforcement agencies. Investigation made clear that the investment firm was bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that - although drug money would be laundered by a payment received from the reinsurer – the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsurer. By offering to pay above market rate the insurer probably intended to assure continuation of the reinsurance arrangement.

- A state insurer in country A sought reinsurance cover for its cover of an airline company. When checking publicly available information on the company it turned out that the

58 FATF Report on Money Laundering and Terrorist Financing Typologies, 2003 – 2004

company was linked to potential war lords and drug traffickers. A report was made to the law enforcement authorities.

Return premiums

There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

- a number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time
- return premium being credited to an account different from the original account
- requests for return premiums in currencies different to the original premium, and
- regular purchase and cancellation of policies.

Over payment of premiums

Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made. A money launderer may well own legitimate assets or businesses as well as an illegal enterprise. In this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally', but on a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be unwilling to confront a customer who is both profitable to the company and important to his own success.

The overpayment of premiums, has, been used as a method of money laundering. Insurers should be especially vigilant where:

- the overpayment is over a certain size (say USD10,000 or equivalent)
- the request to refund the excess premium was to a third party
- the assured is in a jurisdiction associated with money laundering and
- where the size or regularity of overpayments is suspicious.

High brokerage/third party payments/strange premium routes

High brokerage can be used to pay off third parties unrelated to the insurance contract. This often coincides with example of unusual premium routes.

Claims

A claim is one of the principal methods of laundering money through insurance. Outlined below are examples of where claims have resulted in reports of suspected money laundering and terrorist financing.

- A claim was notified by the assured, a solicitor, who was being sued by one of his clients. The solicitor was being sued for breach of confidentiality, which led to the client's creditors discovering funds that had allegedly been smuggled overseas. Documents indicated that the solicitor's client might be involved in tax evasion, currency smuggling and money laundering.

- A claim was notified relating to the loss of high value goods whilst in transit. The assured admitted to investigators that he was fronting for individuals who wanted to invest “dirt money” for a profit. It is believed that either the goods, which were allegedly purchased with cash, did not exist, or that the removal of the goods was organised by the purchasers to ensure a claim occurred and that they received “clean” money as a claims settlement.

- Insurers have discovered instances where premiums have been paid in one currency and requests for claims to be paid in another as a method of laundering money.

- During an on-site visit, an insurance supervisor was referred to a professional indemnity claim that the insurer did not believe was connected with money laundering. The insurer was considering whether to decline the claim on the basis that it had failed to comply with various conditions under the cover. The insurance supervisor reviewed the insurer’s papers, which identified one of the bank’s clients as being linked to a major fraud and money laundering investigation being carried out by international law enforcement agencies.

- After a successful High Court action for fraud, adjusters and lawyers working for an insurer involved in the litigation became aware that the guilty fraudster was linked to other potential crimes, including money laundering.

Assignment of claims

In a similar way, a money launderer may arrange with groups of otherwise legitimate people, perhaps owners of businesses, to assign any legitimate claims on their policies to be paid to the money launderer. The launderer promises to pay these businesses, perhaps in cash, money orders or travellers cheques, a percentage of any claim payments paid to him above and beyond the face value of the claim payments. In this case the money laundering strategy involves no traditional fraud against the insurer. Rather, the launderer has an interest in obtaining funds with a direct source from an insurance company, and is willing to pay others for this privilege. The launderer may even be strict in insisting that the person does not receive any fraudulent claims payments, because the person does not want to invite unwanted attention.

Non-life insurance – fraudulent claims

- Police in Country A uncovered a case of stolen car trafficking where the perpetrators provoked accidents in Country B to be able to claim the damages. The proceeds were laundered via public works companies. A network consisting of two teams operated in two different regions of Country A. Luxury vehicles were stolen and given false number plates before being taken to Country B. An insurance contract was taken out in the first country on these vehicles. In Country B, the vehicles were deliberately written off and junk vehicles with false number plates were bought using false identity documents to be able to claim the damages from the insurance firms in Country A. Around a hundred luxury stolen vehicles were used in this scheme to claim the damages resulting from the simulated or intentional accidents that were then fraudulently declared to the insurance firms. The total loss was over USD 2.5 million. The country in which the accidents occurred was chosen because its national legislation provided for prompt payment of

damages.

On receipt of the damages, the false claimants gave 50% of the sum in cash to the leader of the gang who invested these sums in Country B. The investigations uncovered bank transfers amounting to over USD 12,500 per month from the leader's accounts to the country in question. The money was invested in the purchase of numerous public works vehicles and in setting up companies in this sector in Country B. Investigations also revealed that the leader of the gang had a warehouse in which luxury vehicles used for his trafficking operation were stored. It was also established that there was a business relationship between the leader and a local property developer, suggesting that the network sought to place part of its gains into real estate.[59]

- An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organisation running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of $2 million from similar fraud schemes carried out by terrorist groups.

59 FATF Report on Money Laundering and Terrorist Financing Typologies, 2003 – 2004

Appendix D – List of abbreviations

AML	Anti-money laundering
CDD	Customer due diligence
CFT	Combating the financing of terrorism
FATF	Financial Action Task Force on Money Laundering
FIU	Financial intelligence unit
IAIS	International Association of Insurance Supervisors
ICP	Insurance Core Principle
NCCTs	Non-cooperative countries and territories
PEP	Politically exposed person
STR	Suspicious transaction report