IAIS

INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

APPLICATION PAPER ON COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

OCTOBER 2013

About the IAIS

The International Association of Insurance Supervisors (IAIS) is a voluntary membership organization of insurance supervisors and regulators from more than 200 jurisdictions in nearly 140 countries. The mission of the IAIS is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders and to contribute to global financial stability.

Established in 1994, the IAIS is the international standard setting body responsible for developing principles, standards and other supporting material for the supervision of the insurance sector and assisting in their implementation. The IAIS also provides a forum for Members to share their experiences and understanding of insurance supervision and insurance markets. In addition to active participation of its Members, the IAIS benefits from input in select IAIS activities from Observers representing international institutions, professional associations and insurance and reinsurance companies, as well as consultants and other professionals.

The IAIS coordinates its work with other international financial policymakers and associations of supervisors or regulators, and assists in shaping financial systems globally. In particular, the IAIS is a member of the Financial Stability Board (FSB), founding member and co-parent of the Joint Forum, along with the Basel Committee on Banking Supervision (BCBS) and the International Organization of Securities Commissions (IOSCO), member of the Standards Advisory Council of the International Accounting Standards Board (IASB), and partner in the Access to Insurance Initiative (A2ii). In recognition of its collective expertise, the IAIS also is routinely called upon by the G20 leaders and other international standard setting bodies for input on insurance issues as well as on issues related to the regulation and supervision of the global financial sector.

This paper was prepared by the Financial Crime Working Group of the Market Conduct Subcommittee in consultation with IAIS Members and Observers.

The publication is available on the IAIS website (www.iaisweb.org).

Application paper on combating money laundering and terrorist financing

Contents

Annexes

Introduction

1. The purpose of this paper is to provide information on how money laundering and terrorist financing can occur within the insurance sector, and on measures to mitigate the associated risks. It supplements Insurance Core Principle (ICP) 22 on *Anti-money laundering and combating the financing of terrorism* (AML/CFT) and the accompanying standards and guidance, which apply to insurance supervisors.

2. Within this context this paper provides instructive information that can be used by insurers (including reinsurers) and insurance intermediaries, and is not intended to be exhaustive or prescriptive.

3. 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 and intermediaries can provide the opportunity to launder money or to finance terrorism. Insurers and intermediaries can be involved, knowingly or unknowingly, in money laundering (ML) and the financing of terrorism (FT). The insurance sector should therefore take adequate measures to prevent its misuse by money launderers and those financing terrorism.

4. The IAIS supports the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (FATF Recommendations) issued by the Financial Action Task Force (FATF)[2], as revised in February 2012. The revised FATF Recommendations embody a risk-based approach to AML/CFT. They are applicable at a minimum to the underwriting, placement and administration of life insurance and other investment-related insurance. In addition, they require jurisdictions to consider applying AML/CFT requirements to types of institutions, activities, businesses or professions that, determined through their risk assessments, are at risk of abuse from ML/FT but which do not fall under the definition of financial institution or designated non-financial business or profession (DNFBP). Depending on the conclusion reached by the jurisdiction, some or all of this application paper might be relevant to, for example, the non-life sector. In February 2013 the FATF issued a Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems (the Methodology) and a guidance paper on National Money Laundering and Terrorist Financing Risk Assessment. In October 2009, the FATF published a paper entitled Risk-Based Approach – Guidance for the Life-Insurance Sector. It is expected that a revised version of the paper will be issued by the FATF after 2013.

5. In light of the FATF Recommendations, the IAIS considers there is need for specific information for insurers and insurance intermediaries which is consistent with, and supplements, the FATF standards. This application paper has adopted selected references from the FATF Recommendations, and seeks to encourage their implementation relating to insurers and intermediaries by exploring complementary areas and leveraging the expertise of both organisations. It is not a substitute for consideration of the FATF Recommendations or the Methodology.

1 The insurance sector includes insurers, reinsurers and intermediaries.

2 The FATF is an inter-governmental body which develops international standards and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF works in close cooperation with other entities involved in this area, and in particular FATF associate members and observers. The IAIS has observer status within the FATF.

Money laundering and financing of terrorism in insurance

6. 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 its typology exercises and its Global Money Laundering and Terrorist Financing Threat Assessment.[3]

7. The financing of terrorism can be defined as the wilful provision or collection of funds, by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used in full or in part, to carry out terrorist acts; by a terrorist organisation; or by an individual terrorist.

8. The application of a risk-based approach to FT has both similarities and differences compared to ML. They both require a process for identifying and assessing risk. However, the characteristics of FT mean that the risks may be difficult to assess and the mitigation strategies may be challenging due to considerations such as the relatively low value of transactions involved in FT, or the fact that funds can come from legal sources.

9. Funds that are used to finance terrorist activities may be derived either from criminal activity or may be from legal sources, and the nature of the funding sources may vary according to the type of terrorist organisation. The insurer's or intermediary's responsibility is to report the suspicious activity rather than to determine the type of underlying criminal activity, or intended terrorist purpose. The FIU and law enforcement authorities will then examine the matter further and determine whether there is a link to terrorist financing.

10. Where particular individuals or organisations are the subject of sanctions on terrorist financing (or proliferation financing), the obligations on companies to comply and the listing of those individuals or organisations as a result of such actions are determined exclusively by countries and are not a proper function of traditional risk identification. Violations of such sanctions may result in a criminal offence or sanctions if funds or financial services are made available to a target or its agent.

Vulnerabilities in insurance

11. Life insurance and non-life insurance can be used in different ways by money launderers and terrorist financiers. In assessing risk, the focus should be on the ability and likelihood of a money launderer or terrorist financier to use a particular financial product to store and move illicit funds through the financial system. 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.

12. Money laundering and terrorist financing risks in the insurance industry may be found in life insurance and annuity products. Such products allow a customer to place funds into the financial system and potentially disguise their criminal origin or to finance illegal activities. Life insurance products that can be particularly vulnerable as a vehicle for ML/FT include:

- unit-linked or with profit single premium contracts
- single premium life insurance policies that store cash value
- (second hand) endowment policies.

13. 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

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

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.

14. ML/FT in non-life insurance can occur within the context of, and as the motive behind, insurance fraud, for example where this results in a claim to be made to recover part of the invested illegitimate funds. It could also potentially occur through the cancellation of policies for the return of premium by an insurer's cheque, or the overpayment of premiums with a request for a refund of the amount overpaid.

15. The money laundering approaches outlined above can also be used for terrorist financing. Other examples of how terrorism could be facilitated through non-life 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 terrorists' assets.

16. ML/FT using reinsurance could occur either by establishing fictitious reinsurance companies or reinsurance intermediaries, fronting arrangements and captives, or by the misuse of normal reinsurance transactions. This could 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.

17. Specific cases and examples of money laundering and terrorist financing are included in more detail in Annexes II and III.

The risk-based approach

18. The FATF Recommendations require the adoption of a risk-based approach to combating ML/FT. By adopting a risk-based approach, supervisors, insurers and intermediaries[4] are able to ensure that measures to prevent or mitigate ML/FT are commensurate with the risks identified. This will allow resources to be allocated in the most efficient ways.

19. Adopting a risk-based approach implies the adoption of a risk identification, assessment and management process for dealing with ML/FT risks. This process encompasses recognising the existence of risk, undertaking an assessment of risk, understanding it and developing strategies to manage and mitigate the identified risks.

20. Insurers and intermediaries need to identify higher risk customers, countries[5] or geographic areas, products and services, transactions and delivery channels. In certain cases customers may also be assessed to be lower risk. All relevant risk factors should be considered before determining the level of overall risk, and the appropriate level and type of mitigation to be applied. They should be documented and kept up to date. Assessments are not static. They will change over time, depending on how circumstances develop, and how risks evolve.

21. The strategies to manage and mitigate the identified ML/FT risks in insurance companies and intermediaries are typically aimed at preventing the activity from occurring through a mixture of prevention (e.g. appropriate customer due diligence (CDD) measures), detection (e.g. monitoring and suspicious transaction reporting), and record-keeping so as to facilitate investigations.

4 In October 2009 the FATF published a paper entitled Risk-Based Approach - Guidance for the Life-Insurance Sector. In view of the important service role in the introduction and placement of life insurance and other investment related insurance products played by intermediaries, this FATF paper includes a description of types of contractual relationships between intermediaries and life insurance companies to provide a high-level understanding of the roles played by each.

5 While the ICPs refer to "jurisdictions", this application paper also uses "countries" for consistency with the FATF Recommendations, where appropriate.

22. Appropriate policies, controls and procedures, approved by senior management, should be designed and based on identified and assessed risk. Higher risk areas should be subject to enhanced procedures and other measures: these would include measures such as enhanced CDD checks and enhanced transaction monitoring for higher risk situations. It also follows that in situations where risks are lower, simplified or reduced controls may be applied. The implementation of the policies, procedures and controls will need to be monitored and enhanced as necessary.

Inherent risk assessment

23. A risk-based approach starts with the identification and assessment of the risk that has to be managed. A risk-based approach requires insurers and intermediaries to understand and document the risks of how they might be involved in ML/FT taking into account their customers, countries or geographic areas, products and services, transactions and delivery channels.

24. Insurers and intermediaries 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 inherently 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.

25. Assessing inherent ML/FT risks in business activities involves a process of:

- analysis of ML/FT risks in relation to customers, business relationships, countries or geographic areas, , products, services, transactions and distribution channels, and whether or not the activities in which the risks arise are considered material in value
- assigning appropriate risk levels to, and ranking the relative seriousness of, the risks, and
- highlighting the higher risks among them.

26. The outcome of an inherent risk assessment should be a rational, well-organized and well-documented analysis of risk within each risk category and in combinations of categories that arise in the activities of the insurer or intermediary.

27. Results of the assessment of inherent risks should inform the development or enhancement of due diligence policies and procedures, and the allocation of resources that are commensurate with levels of ML/ FT risk in the activities.

28. Ongoing assessment of inherent ML/FT risks enables insurers and intermediaries to tailor or amend control measures as necessary to address current risk levels, which facilitates the allocation of more risk management resources to areas of greater risk.

Creating customer risk profile categories

29. For an insurer or intermediary to consider the extent of its potential exposure to the risk of ML/FT, it needs to assess the risk of any proposed business relationship. The insurer and intermediary will need to carefully assess the specific background, and other conditions and needs of the customer. To achieve this, the insurer or intermediary will have to collect a range of relevant information,[6] for example details of source of funds, income, employment, family situation, etc.

[6] Subject to relevant data protection laws.

30. Using the inherent risk assessment, the purpose and nature of the business relationship, and any other relevant factors, categories of a customer risk profile should be created prior to the establishment of a business relationship, and maintained throughout the relationship. Based on this assessment, the insurer or intermediary should decide whether or not to accept the business relationship and determine the appropriate level of mitigation to be applied to any risks identified.

31. Factors to consider when creating risk profile categories, 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 and beneficiaries
- the customer's and/or beneficial owner's and beneficiaries' 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 ML/FT or other crime, including whether the customer and/or beneficial owner and beneficiaries are designated by the applicable and relevant United Nations Security Council Resolutions (UNSCRs).

Customer due diligence

32. The FATF Recommendations require insurers and intermediaries to undertake customer due diligence measures including verification of the identity of the customer and beneficial owner when:

- establishing business relationships
- carrying out occasional transactions above the applicable designated threshold (USD/€ 15,000), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked
- there is a suspicion of money laundering or terrorist financing, or
- the insurer has doubts about the veracity or adequacy of previously obtained customer identification data.

The requirements also cover cross-border and domestic wire transfers.[7]

33. The FATF Recommendations prohibit the use of anonymous accounts or accounts in fictitious names. Insurers and intermediaries should identify and freeze without delay the assets of, and otherwise not deal with any designated entities (e.g. terrorists, terrorist

[7] The scope and requirement are set out in the FATF's Interpretive Note to Recommendation 16.

organisations) consistent with their national legislation and the relevant UNSCRs. 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 based on inherent risk assessment results, which, amongst other things address 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.

34. The FATF Recommendations require that the customer due diligence measures taken by insurers and intermediaries include:

(a) identifying the customer (permanent and occasional, natural and legal persons and legal arrangements) and verifying that customer's identity using reliable, independent source documents, data or information ("identification data")

(b) identifying the (ultimate) beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the insurer or intermediary is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding by insurers and intermediaries of the ownership and control structure of the customer

(c) understanding, and as appropriate, obtaining information on the purpose and intended nature of the business relationship and other relevant factors

(d) 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.

When performing elements (a) and (b) insurers and intermediaries also verify that any person purporting to act on behalf of the customer and/or beneficial owner is authorised to do so and identifying and verifying the identity of that person using the identification data described in (a).

35. In addition to the CDD measures required for the customer and the beneficial owner, the FATF Recommendations provide that insurers and intermediaries must conduct the following CDD measures on the beneficiaries of life insurance and other investment related insurance policies as soon as the beneficiaries are identified/designated:

(a) for beneficiaries that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person, and

(b) for beneficiaries that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the insurer or intermediary that it will be able to establish the identity of the beneficiary at the time of the payout.

36. The information collected under (a) and/or (b) should be recorded and maintained in accordance with the record keeping provisions (see paragraphs 129-132).

37. For both cases referred to in 35 (a) and (b) above, the verification of the identity of the beneficiaries should occur at the latest at the time of the payout. In that context the FATF Recommendations require that the beneficiary of a life insurance policy is included as a relevant risk factor by the insurer or intermediary in determining whether enhanced CDD measures are applicable. If the insurer or intermediary determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

38. Where an insurer or intermediary is unable to comply with paragraphs 32-33 above, it should consider making a suspicious transaction report (STR). In cases where insurers or intermediaries form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip off a customer, jurisdictions should permit them not to pursue the CDD process, and instead require them to file a STR.

39. When the identity of customers, beneficiaries and beneficial owners with respect to the insurance contract has been established, the insurer or intermediary is able to assess the risk to its business by checking customers, beneficiaries and beneficial owners against internal and external information on known fraudsters or money launderers (possibly available from industry databases) and on persons listed on publicly available 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 verification will also prevent anonymity of policyholders, beneficiaries and beneficial owners, and the use of fictitious names.

40. Where an insurer or intermediary is unable to comply with relevant CDD measures, the requirements of the FATF Recommendations are that:

- it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship, and
- it should consider making a STR in relation to the customer.

41. Some jurisdictions may choose to include reinsurance within their AML/CFT frameworks. However, 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 identity 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 are supervised for AML/CFT, and have warranted or otherwise confirmed that they apply adequate AML/CFT standards, provided there is no information available to contradict such confirmation. Contradictory information might come from the FATF, trade associations or from the reinsurers' visits to the premises of the insurer.

Existing customers

42. The requirements of the FATF Recommendations for CDD which apply to all new customers and their beneficial owners also apply, on the basis of materiality and risk, to existing customers and their beneficial owners, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained. As to the latter, the insurer or intermediary must conduct due diligence at appropriate times. It may be an appropriate time when a transaction of significance takes place; customer documentation standards change substantially; there is a material change in the relationship; or the institution becomes aware that it lacks sufficient information about an existing customer. In the insurance industry, the various transactions or "trigger events" that occur after the contract date indicate where due diligence should be performed. These trigger events include claims notification, surrender requests, assignments and policy alterations, such as changes in beneficiaries (see also paragraph 81).

43. If during the establishment or course of the business relationship, or when conducting occasional transactions, an insurer or intermediary suspects that transactions relate to ML/FT, then the insurer or intermediary should:

- seek to identify and verify the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply, and
- make a STR to the Financial Intelligence Unit (FIU).

Methods of identification and verification

44. This section 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 and intermediaries. Since, however, this paper is neither mandatory nor exhaustive, there may be cases where an insurer or intermediary 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.

45. Reliable and independent identification data should be obtained from each verification subject. "Reliable and independent" means that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

Individuals

46. The personal information used to identify the customer may include:

- full name(s) and alias used
- date and place of birth
- nationality
- current permanent address[8] including postcode/zipcode
- occupation and name of employer (if self-employed, the nature of the self-employment)
- specimen signature of the individual.

47. It is recognised that different jurisdictions have different identification documents. In order to verify identity it is suggested that the following documents may be considered to be the best possible:

- current valid passport, or
- national identity card.

48. However, some jurisdictions do not have national identity cards and many individuals do not possess passports. Some jurisdictions establish criteria in respect of acceptable verification documents, taking into account local conditions. Identity should always be verified using reliable, independent source documents, data or information.

49. 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 should certify the authenticity of the copies.

Legal persons, companies, partnerships, other institutions and arrangements

50. When performing CDD measures in relation to customers that are legal persons or legal arrangements (see selected FATF definitions in Annex I), the FATF Recommendations require insurers or the intermediary to identify and verify the customer, and understand the nature of its business, and its ownership and control structure.

51. The insurer or the intermediary should:

a) Identify the customer and verify its identity – the types of measures that would normally be needed to perform this function satisfactorily would require obtaining and verifying the following information:

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

- name, legal form and proof of existence – for example through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable, independent source proving the name, form and current existence of the customer
- the powers that regulate and bind the legal person or arrangement e.g. the memorandum and articles of association of a company as well as the names of the relevant persons having a senior management position in the legal person or arrangement; (see also paragraph 46)
- the address of the registered office and main place of business.

b) Identify the beneficial owners and take reasonable measures to verify the identity of such persons through the following information:

- for legal persons
  - (i) the identity of the natural persons, (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership), who ultimately have a controlling ownership interest in a legal person, and
  - (ii) to the extent that there is doubt under (i) as to whether the person(s) with the controlling ownership[9] interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.
  - (iii) Where no natural person is identified under (i) or (ii) above, insurers and intermediaries should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.
- for legal arrangements:
  - (i) that are trusts, the identity of the settlor, the trustee(s), the protector (if any) and the beneficiaries/class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership)
  - (ii) that are other types of legal arrangement, the identity of persons in equivalent or similar positions.

52. Where the customer or the owner of the controlling interest is a company listed on a stock exchange and is subject to regulatory disclosure requirements (either by stock exchange rules or through law or enforceable means) which ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of that company. The relevant information or data may be obtained from a public register, from the customer or from other reliable sources. This provision could also apply to mutual insurance companies and fraternal benefit societies that are subject to similarly rigorous levels of regulatory oversight as insurers listed on a stock exchange.

[9] The FATF Methodology describes controlling ownership as follows "A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%)."

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

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

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

56. 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.

57. The FATF Recommendations require insurers and intermediaries to maintain their records with respect to legal persons and legal arrangements in such a way as to enable competent authorities to access adequate, accurate and current information on the beneficial ownership and control of legal persons and legal arrangements, and in particular the settlor, the trustee and the beneficiaries of express trusts, in a timely way.

High risk relationships

58. The FATF Recommendations require enhanced CDD measures, consistent with the risks identified, to be taken with respect to all higher risk categories of business relationship, customer and transactions.

59. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc), and updating more regularly the identification data of customer and beneficial owner
- obtaining additional information on the intended nature of the business relationship
- obtaining information on the source of funds or source of wealth of the customer
- obtaining information on the reasons for intended or performed transactions
- obtaining senior management approval to commence or continue the business relationship
- conducting enhanced ongoing monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Assessing the ML/FT risks in higher risk cases

60. Examples of situations where customer or, business relationship risk could be higher include the following:

- the business relationship is conducted in unusual circumstances e.g. significant unexplained geographic distance between the insurer or intermediary and the customer
- the business is cash intensive
- customers are non-resident
- legal persons or arrangements that are personal asset holding vehicles
- companies have nominee shareholders or shares in bearer form
- the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

61. The country or geographic risk factor should always be considered as higher for countries that insufficiently apply the FATF Recommendations and which are identified by FATF Statements that call on countries to take action (see paragraphs 64 and 65 below). Other examples where country or geographic risk could be higher include:

- countries identified by credible sources such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems
- countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations
- countries identified by credible sources as having significant levels of corruption, or other criminal activity
- countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within them.

62. Examples of situations where the product, service, transaction or delivery channel risk factors could be higher include:

- large cash or other forms of anonymous transactions
- non-face-to-face business relationships or transactions (i.e. the carrying out of an insurance contract, without the simultaneous physical presence of the insurer or intermediary and the consumer, by making exclusive use of one or more of the internet, telemarketing, or other electronic means of communication up to and including the time at which the contract is concluded)
- payments received from unknown or un-associated third parties.

63. Other types of business relationships which should be assessed as high risk and be subject to enhanced CDD measures are mentioned in the following paragraphs.

Higher risk countries

64. Insurers and intermediaries are required by the FATF Recommendations to apply enhanced CDD to business relationships and transactions with natural and legal persons,

and financial institutions, from countries for which this is called for by the FATF.[10] The type of enhanced CDD measures applied should be effective and proportionate to the risks.

65. In specific circumstances, jurisdictions may be asked by the FATF to impose appropriate countermeasures. Jurisdictions may also apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks. There should be effective arrangements in place to ensure that insurers and intermediaries are advised of these.

Bearer policies

66. Bearer policies are insurance contracts 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 needing to seek the 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 transferred 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 strongly discouraged, not least because of the importance of performing enhanced CDD combined with the inherent uncertainties in being able to undertake CDD on the beneficiaries.

Viatical arrangements

67. 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". In light of the inherent risks, where viatical arrangements are allowed in a jurisdiction, supervisory overview or regulation is strongly 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.

Simplified customer due diligence in lower risk cases

68. The FATF Recommendations require the full range of CDD measures to be applied to the customer (including the requirement to identify the beneficial owner) and business relationship. However, if the risk of money laundering or the financing of terrorism is lower (based on an adequate analysis of the risks by the insurer or intermediary, or by the country) it could be reasonable for insurers and intermediaries to apply, subject to national legislation and guidelines, simplified CDD measures when identifying and verifying the identity of the customer, the beneficial owner and other parties to the business relationship.

69. Examples of where the customer risk factor could be lower are:

[10] For instance jurisdictions may be publicly identified in one of the two FATF public documents that are issued three times a year:

The first public document, the *FATF's Public Statement*, identifies:

1) jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures apply

2) jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies.

In the second FATF public document, *Improving Global AML/CFT Compliance: On-going Process*, the FATF identifies jurisdictions with strategic AML/CFT deficiencies that have provided a high-level political commitment to address the deficiencies through implementation of an action plan developed with the FATF.

More information can be obtained from the FATF website: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

- financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and the financing of terrorism consistent with the FATF Recommendations, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements
- public companies listed on a stock exchange and subject to regulatory disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company
- public administrations or enterprises.

70. Examples of circumstances where the product, service, transaction or delivery channel risk factor could be lower are:

- life insurance policies where the annual premium is less than USD/€ 1000 or a single premium of less 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
- financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

71. Examples of situations where the country risk factor could be lower are where:

- countries are identified by credible sources such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems
- countries are identified by credible sources as having a low level of corruption, or other criminal activity.

72. In making a risk assessment, insurers or intermediaries could, when appropriate, also take into account possible variations in ML/FT risk between different regions or areas within a country.

73. The simplified CDD measures should be commensurate with the lower risk factors. It does not automatically mean that the same customer is lower risk for all types of CDD measures, e.g. the simplified measures could relate only to customer acceptance measures or to aspects of on-going monitoring. Examples of possible measures are:

- verifying the identity of the customer and the beneficial owner after the establishment of the business relationship e.g. if account transactions rise above a defined monetary threshold
- reducing the frequency of customer identification updates
- reducing the degree of on-going monitoring and scrutinising transactions based on a reasonable monetary threshold, and
- not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

74. However, the FATF Recommendations provide that:

- simplified CDD measures are not acceptable in any event when there is a suspicion of money laundering or terrorist financing or specific higher risk scenarios apply, and
- the extent of risk sensitive CDD measures taken by insurers and intermediaries must also be consistent with national legislation and guidelines issued by the competent authorities.

Timing of identification and verification

75. The FATF Recommendations require insurers and intermediaries to undertake CDD measures before or during the course of establishing the business relationship with that person. More specifically, they require insurers to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship. 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.

76. Where a policyholder and/or beneficiary is permitted to utilise the business relationship prior to verification, the FATF Recommendations require insurers and intermediaries to adopt risk management procedures concerning the conditions under which this may occur. These procedures should include measures such as a contractual limitation on 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.

77. The FATF Recommendations recognise that identification and verification of the identity of the customer and beneficial owner may (if permitted) take place after the establishment of the business relationship provided that:

- this occurs as soon as reasonably practicable
- it is essential not to interrupt the normal conduct of business, and
- the money laundering risks and financing of terrorism risks are effectively managed.

78. Where the insurer or intermediary has already commenced the business relationship and is unable to comply with the verification requirements, the FATF Recommendations require it not to conduct further transaction, or to terminate the business relationship and consider making a STR. An insurer or intermediary that has not commenced business relations or performed a transaction, and is unable to comply with the verification requirements, must not commence business relations or perform the transaction and it must consider making a STR.

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

- group pension schemes
- non-face-to-face customers (such as those using internet, telemarketing, or other electronic means of communication)
- premium payment made before the application has been processed and the risk accepted
- using a policy as collateral.

Ongoing due diligence and monitoring

80. The FATF Recommendations require the insurer or intermediary to perform ongoing due diligence on the business relationship. Ongoing due diligence must include scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile category, and where necessary, the source of funds. There should also be systems to detect prohibited (e.g. with entities designated by the relevant UNSCRs), unusual or suspicious transactions, and investigate them as required. The insurer or intermediary should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. It should assess whether the change/transaction fits the risk profile category of the customer and/or beneficial owner or is for some other reason unusual or suspicious.

81. Examples of transactions or trigger events after establishment of the contract that require CDD review 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.

82. The above list is not exhaustive; insurers and intermediaries should consider other types of transactions or trigger events which are appropriate to their type of business. It should also be noted that some of the above events can be expected over the life of a contract and are not necessarily suspicious.

83. Occurrence of these transactions and events does not imply that (full) CDD 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 the information it holds. As an example, doubts might arise if benefits from one policy of insurance are used to fund the

premium payments of another policy of insurance or where there is a suspicion of money laundering or financing of terrorism in relation to that customer.

84. The CDD programme should be established in such a way that the insurer or intermediary is able to adequately gather and analyse information. The FATF Recommendations require insurers and intermediaries to ensure that documents, data or information gathered under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

Politically exposed persons

85. The FATF Recommendations require enhanced due diligence measures to be taken in relation to foreign politically exposed persons (PEPs).[11] For this purpose insurers and intermediaries must:

(a) have appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner of a customer is a foreign PEP

(b) obtain senior management approval for establishing (or continuing for existing customers) such business relationships

(c) take reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners identified as PEPs, and

(d) conduct enhanced ongoing monitoring of the business relationship.

86. The FATF requires insurers and intermediaries also to take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with a domestic PEP, insurers and intermediaries must apply the measures referred to in (b), (c) and (d) above.

87. In addition, the FATF Recommendations require that reasonable measures are taken to determine whether the beneficiary of a life insurance policy and/or where required, the beneficial owner of the beneficiary is a PEP. This should occur at the latest at the time of the payout. In addition to performing normal CDD measures, where higher risks are identified, insurers and intermediaries must:

- inform senior management before the payout of the policy proceeds, and
- conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious transaction report.

88. The requirements for all types of PEP also apply to family members or close associates of such PEPs.

89. Insurers and intermediaries may use a number of ways to assist with the identification of PEPs. These could include using internet and media searches, commercial databases, PEP-lists from government authorities (if available), in-house databases, asset disclosure systems, customer self declarations etc. Regardless of the means used to identify PEPs, insurers and intermediaries should adopt commensurate measures, and be satisfied that they have taken adequate steps to comply with the relevant CDD requirements.

[11] In June 2013 the FATF issued a Guidance paper on Politically Exposed Persons, to provide non-binding guidance to assist competent authorities aand financial institutions and DNFBPs to effectively implement Recommendations 12 and 22.

New or developing technologies

90. The FATF Recommendations require insurers and intermediaries to identify and assess the ML/FT risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. Insurers and intermediaries should undertake this assessment prior to the launch of the product, practice or technology, and should take appropriate measures to manage and mitigate the risks identified.

91. New or developing technologies can be used to market insurance products. E-commerce or selling over the internet is an example of this. Insurers and intermediaries that use new and developing technologies should include these in the inherent risk assessment process, to ensure in turn that appropriate AML/CFT controls are implemented and maintained around them.

Reliance on third parties[12]

92. Depending on the legislation of the jurisdiction in which the insurer operates, it may be allowed to rely on third parties to perform elements (a)–(c) of the CDD measures set out in paragraph 34.

93. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the insurer relying on the third party.

94. Where such reliance, or reliance for the purpose of introducing business, is permitted, the FATF Recommendations require that the following criteria be met:

(a) insurers relying on a third party immediately obtain from the third party, the necessary information concerning elements (a)–(c) of the CDD measures set out in paragraph 34

(b) insurers 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 third party upon request without delay, and

(c) insurers satisfy themselves that the third party is regulated, supervised or monitored for and has measures in place for compliance with, CDD and record-keeping requirements in line with FATF Recommendations 10 (customer due diligence) and 11 (record keeping).

95. The FATF Recommendations require that reliance on a third party take into consideration the information available (e.g. whether the FATF has called for enhanced due diligence measures or countermeasures to be applied) on the level of country or geographical risk of the jurisdictional in which the third party is based. Insurers and intermediaries should likewise consider information about these risks and where appropriate restrict their use of such third parties.

96. The FATF has also crafted similar provisions in respect of financial groups. Where an insurer relies on a third party that is part of the same financial group, and the following are met:

(a) the group applies CDD and record-keeping requirements, in line with Recommendations 10 (customer due diligence), 11 (record keeping) and 12 (politically exposed persons), and programmes against money laundering and terrorist financing, in accordance with Recommendation 18 (internal controls and foreign branches and subsidiaries)

12 The following paragraphs 92-99 do not apply to outsourcing or agency relationships other than relationships with insurance agents and brokers, i.e. they do not apply where the agent is acting under a contractual arrangement with the insurer to carry out its CDD functions.

(b) the implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, and

(c) any higher country risk is adequately mitigated by the group's AML/CFT policies,

then the criteria of 94 (a) to (c) above could be considered met through its group programme.

97. The checks by the insurer do not have to consist of a check of every individual transaction by the intermediary or other third party; however, the insurer must be satisfied that the AML/CFT measures are implemented, are operating adequately, are at least equivalent to their own legal and regulatory requirements, and comply with the CDD and record keeping requirements of FATF Recommendations 10 and 11.

98. Insurers should satisfy the above provisions by way of contractual agreement or other documentation with third parties, and by enforcement of the terms. Specific clauses should include commitments by third parties regarding performance of the necessary CDD measures, complete and up-to-date record keeping, granting access to client files and sending (copies of) files to the insurer upon request within required timeframes and without delay. The agreement could also include other commitments, such as reporting to the FIU and the insurer in the case of a suspicious transaction or attempted suspicious transaction. It is recommended that insurers use application forms to be filled out by the customers and third parties that include information on identification of the customer and the beneficial owner(s), and on third party and PEP determination, as applicable, as well as the method(s) used to verify identity. Insurers should periodically review, in a systematic manner, the quality of client information gathered and documented, to ensure their requirements continue to be met.

99. If the insurer has any doubts about the ability of the intermediary or other third party to undertake appropriate due diligence, or about the performance of due diligence responsibilities, it should undertake and complete its own CDD, including verification of identities and other collected information. Insurers should consider terminating relationships with intermediaries and other third parties who do not comply with agreed upon responsibilities or provide the requisite information to the insurer on a timely basis.

100. The extent of the insurer's exposure to the third party should be addressed expressly in the insurer's inherent risk assessment.

Suspicious transaction reporting[13]

101. If an insurer or intermediary suspects, or has reasonable grounds to suspect, that funds are the proceeds of a criminal activity, or are related to terrorist financing,[14] the FATF Recommendations require that it reports its suspicions promptly to the FIU (by means of a STR). All suspicious transactions, including attempted transactions, must be reported regardless of the amount of the transaction or whether they are thought, among other things, to involve tax matters. Insurers and intermediaries should also take note of other reporting obligations in their jurisdiction, including those relating to assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs.

102. An important pre-condition of recognition of a suspicious transaction is for the insurer or intermediary to know enough about the customer and business relationship to recognise that a transaction, or a series of transactions, is unusual. This is facilitated through ongoing CDD and monitoring processes.

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

14 Terrorist financing here refers to the financing of terrorist acts, and also terrorist organisations or individual terrorists, even in the absence of a link to a specific terrorist act or acts.

103. Suspicious transactions might fall into one or more of the following non-exhaustive 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 apparently 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.

104. 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.

105. The FATF Recommendations provide that insurers and intermediaries, their directors, officers and employees (permanent and temporary) must not disclose the fact that a STR is being made or related information is being reported, or has been reported, to the FIU. A risk exists that customers could be unintentionally tipped off when the insurer or intermediary is seeking to perform its CDD obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspect ML/FT operation.

106. Therefore, if insurers and intermediaries form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off when performing the CDD process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file a STR. Insurers and intermediaries should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD.

Internal controls and foreign branches and subsidiaries

107. The FATF Recommendations require insurers and intermediaries to have in place and implement programmes and systems to prevent money laundering and the financing of terrorism.

108. The FATF Recommendations require these programmes to include internal policies, procedures and controls which have regard to the risk of ML/FT and the size of the business, and which cover:

(a) appropriate compliance management arrangements, including the appointment of an AML/CFT compliance officer[15] at the management level

(b) adequate screening procedures to ensure high standards when hiring employees

15 The term 'compliance officer' may in some jurisdictions be referred to as the money laundering reporting officer or chief anti-money laundering officer, or similar. The compliance officer would have responsibility for on-going monitoring of the fulfilment of AML/CFT duties by the insurer, and act as the contact point regarding AML/CFT issues, both internal and external, including reporting suspicious transactions. To carry out these responsibilities effectively the compliance officer should have sufficient resources. The compliance officer would also need to be sufficiently independent from other business functions to ensure that AML/CFT concerns are raised with and addressed objectively by the insurer's Board.

(c) an ongoing employee training programme

(d) an independent audit function to test the AML/CFT system.

109. The training programme could include information on new developments; information on current ML/FT techniques, methods and trends; and a clear explanation of all aspects of AML/CFT laws and obligations, and in particular, requirements concerning CDD and suspicious transaction reporting. Internal audit could include sample testing.

110. Internal policies, procedures and controls could usefully cover all aspects of AML/CFT programmes of insurers and intermediaries, such as:

(a) CDD

(b) the detection of unusual or suspicious transactions and the reporting obligations

(c) record keeping and record retention arrangements

(d) the communication of policies, procedures and controls to the employees.

111. Each programme should be sufficiently robust to handle the volume of information processed by that insurer or intermediary effectively and efficiently. The programmes and systems should constitute an operational, practical and precise approach for dealing with ML/FT risks. These programmes and systems should be adapted to the group, its organisational (e.g. joint back office) and responsibility structures, and to products and market conditions. The development of policies, procedures and controls enables the insurer and intermediary to comply with their AML/CFT obligations and to determine the standard of CDD that is suitable for its own organisation. It is also important 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.

112. It is important that the board of directors and senior management of the insurer or intermediary should not only establish and support the development of internal policies, procedures and controls but should also ensure that they are properly implemented and adhered to. Implementation of internal AML/CFT measures should constitute a relevant priority to insurers and intermediaries. 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 or intermediary 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.

113. 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 have sufficient independence and resources to investigate and verify the details in order to determine whether the insurer or intermediary should submit a report to the FIU. The compliance officer should keep adequate records of all such reports and investigations, including a register of all reports to the FIU and a separate register of all reports made to him by staff.[16]

114. Insurers and intermediaries 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 investigating and reporting suspicions of money laundering and the financing of terrorism without delay to the FIU, and

16 Including agency and temporary staff.

- all staff know to whom their suspicions should be reported.

Some jurisdictions require that a specified compliance officer (for example a Money Laundering Reporting Officer) is responsible for reporting all suspicions reported to him/her via internal procedures.

115. The FATF also requires financial groups to implement group-wide programmes against money laundering and terrorist financing, which should be applicable, and appropriate, to all branches and majority-owned subsidiaries of the financial group. These should include the measures set out in criterion 18.1 of the FATF Methodology (see paragraph 108), and also:

(a) policies and procedures for sharing information required for the purposes of CDD and ML/FT risk management

(b) the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes, and

(c) adequate safeguards on the confidentiality and use of information exchanged.

116. In the case of foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, the FATF requires that insurers and intermediaries ensure that their branches and majority owned subsidiaries implement the AML/CFT requirements of the home jurisdiction to the extent that local (i.e. host country) laws and regulations permit. Insurers must pay particular attention that this principle is observed with respect to their branches and subsidiaries in jurisdictions identified as higher risk countries by the FATF. Where local applicable laws and regulations prohibit this implementation, or where the host country otherwise does not permit the proper implementation of AML/CFT measures consistent with home country requirements, insurers and intermediaries should apply appropriate additional measures to manage the ML/TF risks and inform the supervisor in the jurisdiction of the parent institution that it cannot apply the group-level AML/CFT programmes and FATF Recommendations for this reason.

117. It is recommended that insurers, intermediaries and other financial institutions liaise to exchange information both on 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.

Screening and training of staff

118. In order to meet the FATF Recommendations staff should have the level of competence necessary for performing their duties. Insurers and intermediaries 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.

119. Insurers and intermediaries 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 124 to 128 provide a description of relevant positions.

120. The responsibility for initial and on-going assessment of the fitness and propriety of staff lies with the insurer or intermediary. 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.

121. 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.

122. Insurers and intermediaries 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.

123. The FATF Recommendations require the staff of insurers and intermediaries to receive initial and ongoing training on relevant AML/CFT legislation, regulations and guidance, and the insurers' own AML/CFT policies and procedures. Although each insurer and intermediary 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 would be expected to include at a minimum:

- a description of the nature and processes of money 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, regulations and guidance
- a general explanation of the insurers' AML/CFT policy and systems, including particular emphasis on verification, the recognition of suspicious customers/transactions and the need to report suspicions to the compliance officer.

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

125. 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.

126. They need to be made aware of their legal responsibilities and the AML/CFT and all other relevant policies and procedures of the insurer or intermediary. They need to be aware, in particular, of the client acceptance policies, 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 policies and procedures.

127. 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, regulations and guidance including the offences and penalties arising from breaches of the requirements
- procedures relating to the service of production and restraint orders (to stop writing business)
- internal reporting procedures,
- the requirements for CDD verification and record keeping.

128. 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 should have adequate skills and resources and will require extensive initial and continuing instruction on the validation and reporting of suspicious customers/transactions and freezing assets in accordance with the relevant legislation.

Record keeping and retention

129. The FATF Recommendations require insurers and intermediaries to maintain records of the identification data and other records obtained through CDD measures, and to retain them for at least five years following the end of a business relationship (or longer if requested by a competent authority in specific cases and upon proper authority). Records would include client, policy or other account files, business correspondence, and the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual or large transactions). This would include information on the risk profile of each customer and/or beneficial owner and the data obtained through the CDD process, such as the customer's (and beneficiary's) name, address (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, the type and identifying number of any account involved in the transaction, and official identification documents (such as passports, identity cards or similar documents). For insurers this implies that there are prescribed periods for keeping relevant records for at least five years after the expiry of policies.

130. The FATF requires insurers and intermediaries also to maintain all necessary records on transactions, both domestic and international, for at least five years after completion of the transaction (or longer if requested by a competent authority in specific cases and upon proper authority). This requirement applies regardless of whether the business relationship is ongoing or has ended. Transaction records must be sufficient to permit reconstruction of individual transactions (including the amount and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

131. Insurers and intermediaries 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".

132. The FATF Recommendations require all customer identification data, other CDD information, transaction records and other relevant information to be available on a timely basis to the AML/CFT compliance officer and other appropriate staff. Such data and information should be available on the same basis to appropriately entitled domestic competent authorities.

SELECTED FATF DEFINITIONS

The definitions in this annex are taken from the glossary of definitions which forms part of the FATF Recommendations and are applicable only to the AML/CFT requirements of ICP 22.

Beneficial Owner

Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer[17] and/or the natural 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.

Beneficiary

The meaning of the term *beneficiary* in the FATF Recommendations depends on the context:

- In trust law, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period.
- In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy.

- Financial Group
- Financial group means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.

Financial institution

Financial institutions means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.
2. Lending.
3. Financial leasing.
4. Money or value transfer services.
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.

17 This definition also applies to beneficial owners of beneficiaries under a life or other investment linked insurance policy.

7. Trading in:
    (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.);
    (b) foreign exchange;
    (c) exchange, interest rate and index instruments;
    (d) transferable securities;
    (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance.
13. Money and currency changing.

International Organisations

International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.

Legal Arrangements

Legal arrangements refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.

Legal Persons

Legal persons refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

Politically Exposed Persons

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by 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.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, 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.

Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

MONEY LAUNDERING CASE STUDIES

Life policies – case study 1

Mrs T (teacher) from country A, entered into a life insurance policy with a small initial premium being paid. The transaction was arranged by Mr B who was the agent of insurance company C and a cousin of Mrs T. Two days later, company C made a payment of an additional premium, in excess of €540,000, on behalf of Mrs T. After one month, Mrs T cancelled her policy and transferred the refund of contributions to three different accounts:

a) Mr MD (Managing Director of Company C) – €240,000;

b) Mrs N (niece of Mr MD) – €150,000; and

c) Mr U – €150,000.

All of them subsequently transferred the money onwards to other accounts in different banks. Following an investigation it appeared that the money being laundered was linked to fuel smuggling. The accounts were blocked by the Financial Intelligence Unit (FIU) and the case was forwarded to the public prosecutor.

Life policies – case study 2

A single premium on a life policy, totalling more than €500,000 was paid on behalf of Mr A by Mr A's employer, who was a related person. Half of the amount was withdrawn by Mr A within a month of paying the premium. A request for withdrawing the balance of the amount was filed at the same time.

Following a report to the FIU subsequent checks revealed that Mr A had a criminal record and was involved in pending legal proceedings. It also appeared that Mr A was allegedly involved in drug dealing and assassinations. Following further investigation and collection of information, including tax records, and movements of funds on Mr A's accounts the relevant information was forwarded to law enforcement agencies.

Life policies – case study 3

A life insurance policy with a very high single premium included a clause for partial redemption, at the client's request, at the end of each year. The client claimed that the purpose of the clause was to repay the interest on a loan with a duration of 10 years, intended to facilitate the building of a warehouse. The insurer reported a suspicion to the local FIU because of the high premium and because the client refused to name the bank where he had taken up the loan. After careful examination by the FIU, it turned out that the client was known to the police as he had committed financial fraud. It appears that the client had tried to launder money by means of a life insurance product.

Life policies – case study 4

An insurance company filed a report of suspicion concerning two foreign individuals each of whom bought a single premium life insurance contract. The premiums were very high. The investigation by the FIU showed that the premiums for these insurance policies were paid through the current accounts of the two clients, while payments to the accounts consisted of cash deposits the origin of which was unknown. Moreover, the accounts were only used for payment for the insurance policy and the account holders had already been the subject of a report on illegal drug trafficking. According to the police reports, the individuals were members of a network responsible for trafficking drugs from Latin America to Western Europe. The insurance company reported suspicion of potential money laundering on the basis of several factors, namely that the policyholders did not have an official address in the country where they wanted to buy the policy, they were not exercising any professional

activity in that country, and they could not explain the origin of the money. This case is currently subject to legal proceedings.

Life policies – case study 5

Mr A, who claimed to be a 25 year old garage owner, bought a life insurance policy with a high single premium in relation to his age. The policy was issued for a duration of 10 years with Mr A being the beneficiary if alive and Mrs B being the beneficiary in the case of the death of Mr A during the 10 year duration of the policy (Mrs B being the grandmother of Mr A). The insurance company reported the case to the FIU. Research by the FIU showed that Mr A did not own a garage but had been involved in drug trafficking. The FIU forwarded its report to the department of justice, which dealt with cases of drug trafficking.

Life policies – case study 6

A couple in their twenties purchased several single premium life insurance contracts with the same insurance company. A little later they requested an early repayment of these policies in cash. This, combined with the young age of the insured, attracted the attention of the insurance company. The FIU found that both policyholders had convictions and were the subjects of a drug investigation. The file was referred to the criminal court.

Life policies – case study 7

A policyholder living abroad bought a life insurance policy and, soon afterwards, requested early surrender of the policy. This early surrender resulted in high costs for the policyholder. Afterwards, the policyholder made a request by fax to transfer the money to an account of another person living abroad. The insurer contacted the FIU, which, in light of the urgency of the situation, requested that the transaction should be postponed for 24 hours. This gave the FIU time to collect data, which indicated that the policyholder had been convicted for illegal public attraction of savings. The case has been transferred to the justice department for further investigation.

Life policies – case study 8

Two life insurance policies were bought for a large amount in the names of Mr X and Mr Y. The payments were made by cheque, originating from the account of a European investment company. Both polices were used as security for a mortgage loan with a company that specialised in leasing. As the beneficiaries were not the policyholders and in light of the unusual financing being provided by a leasing company, the insurer contacted the investment company in order to understand the origin of the money that had been deposited in the account. It appeared that the money was deposited with the company in cash by random clients. Following the disclosure of suspicion by the insurance company it became evident that Mr X and Mr Y were known by the customs authorities for the illegal importation and exportation of cars.

Life policies – case study 9

A 34 year old car dealer received a loan through a broker of a life insurance company to purchase a house. He invested around 25% of the loan in a single-premium life insurance policy. He later surrendered the policy early to pay back the loan (capital and interest), making up the shortfall through other funds. The use of a substantial proportion of the loan to purchase a policy combined with the unexpectedly early repayment of the loan led to the FIU being contacted. The FIU's investigation revealed that the policyholder was known for stealing and receiving stolen cars. Moreover, he had used false documents to prove the sources of his income and wealth.

Life policies – case study 10

A life insurance company was contacted by a financial adviser calling on behalf of a customer who had taken out a policy. The customer had recently been convicted of fraud and wished to ascertain whether such a conviction would compromise the policy's terms and conditions. The conviction did not pose a problem for the continuation of the policy. However the disclosure of fraud prompted an internal review. Active investment policies were identified and a media article was found, which stated that the customer had been part of a gang involved in a €6 million tax fraud and subsequent money laundering offences. A suspicious activity report was submitted to the FIU. Following dissemination of the intelligence by the FIU, the tax authority advised the insurance company that its report provided useful information, allowing a case for confiscation of assets to be made.

Life policies – case study 11

A life insurance company in Country A, which had sold a substantial investment policy to Mr J, was approached by the police force. Mr J was being investigated as he was part of a criminal gang trafficking heroin from Country F by using sophisticated processes to assimilate heroin into cardboard boxes, which were subsequently used to ship legitimate cargo overseas. Once the contents of the boxes had been delivered, the empty boxes were taken to a processing plant in a window manufacturing business, where the heroin was removed, processed, and sold. Mr J had purchased the policy by means of a very large transfer from his bank account citing the source of funds in the account as the product of savings and income. After a review, it was found that the relationship with the insurer had been structured so that it contained cross-border elements which facilitated money laundering, including the fact that the investment was an overseas product promoted by the company.

Life policies – case study 12

A life insurance company received a payment of €25,000 for an existing customer via an 'over the counter' transaction. When the money was received, enquiries were made by the company as to where the money had come from. It transpired that the money had been deposited in cash at a bank in order to pay premiums to the insurance company. The receiving bank had not asked questions when the cash was received. However, the life insurance company considered the transaction to be suspicious in light of the amount, the fact that it had not received such a payment from the customer before and that it contradicted confirmations provided by the customer as to how payments would be made, and the absence of reasonable responses by the customer to questions by the insurance company. Consequently, a suspicious activity report was made to the FIU.

Life policies – case study 13

A financial adviser approached a life insurance company in order to make a pre application enquiry on behalf of a prospective customer to PEP classifications and other issues. The potential applicant was married to a former president of a developing country who was in self-imposed exile due to outstanding criminal matters. The spouse was seeking a whole life product in order to protect her tax liabilities. However, the husband was implicated in a multi-million dollar theft of public state money. The business was rejected and a report made to the FIU.

Life policies – case study 14

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 USD1.1 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 USD1.2 million and represented the last step in the laundering operation.

Life policies – case study 15

A husband and wife took out a life insurance policy each in their own name with annual premiums. In the event of the death of one of the spouses, the other spouse would become the beneficiary of the insurance. The holder of the account through which the premiums had been paid was found not to be the policyholders but a company abroad of which they were directors. However, this was a life insurance policy taken out privately by the couple and not by the company. Investigation revealed that the scenario set up had been intended to conceal the illicit origin of the funds which originated from serious and organised tax fraud for which the couple involved was known.

Life policies – case study 16

A fraudulently bankrupt subject used an account in the name of a family member to pay cash in and withdraw it out via a cheque to a lawyer. The lawyer then gave some money back in a cheque to the family member while the rest went to the subject's single premium life policy which was immediately surrendered. The surrender value was paid out to the family member's account.

Non-life – case study 17

Numerous motor vehicles owned by a number of companies were insured. As part of the process for setting up the insurance policies various company documents were reviewed by the insurer. The companies had been incorporated during 1994-1995 when Mr X was 24 years old. The registered business activities of the companies set out significant investments that did not correspond to the age and status of Mr X. The companies appeared to be linked to other persons related to Mr X and were incorporated with the same address. Subsequently Mr X refused to provide information on the origin of the funds used to acquire the motor vehicles. A report was submitted to the FIU and an investigation was instigated.

Non-life – case study 18

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.

Intermediaries – case study 19

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 raised no suspicion at the bank, since the insurance broker was known to them as being connected to the insurance branch. The insurance

broker delivered, 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 raising suspicions with the insurance company.

Intermediaries – case study 20

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.

Collusion – case study 21

An insurer in collusion with an insured person attempted to launder money through insurance transactions. The manager of an insurance company sold health and personal injury insurance policies insuring against the liability from accidents to dummy persons, normally in the names of friends and relatives. These persons paid a low premium rate. Subsequently claims were received, supported by false documentation and medical certificates to substantiate the losses and the insurer paid the claims promptly. The claims for damages were considerable. The manager then sought to legalise this scheme and recover the damages paid out. Under subrogation rights, the insurance company took legal action against all businesses where the alleged accidents had occurred. The businesses involved (restaurants, clubs etc.) responded that they had not been aware of the alleged accidents and that no such accidents had occurred at the times stated.

Collusion – case study 22

A drug trafficker purchased a life insurance policy with a value of USD 80,000. The policy was purchased through an agent of a large life insurance company using a cashier's cheque. The investigation showed that the client had made it known that the funds used to finance the policy were the proceeds of drug trafficking. In light of this fact, the agent charged significantly higher commission. Three months following this transaction, the investigation showed that the drug dealer cashed in his policy.

Reinsurance – case study 23

An insurer in Country A sought reinsurance with a reputable reinsurance company in Country B for its directors and officers 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.

Reinsurance – case study 24

A group of persons with interests in home construction effected a payment in favour of construction company A under contracts connected with their participation in investment

construction (at cost price). Insurance company P accepted possible financial risks to these contracts under a contract of financial risks insurance and received an insurance premium. At the same time the insurance company P concluded with the construction company A a secret agreement providing that the difference between the market cost of housing and the cost price was transferred in favour of the insurance company as a premium under the contract of financial risks insurance. When the funds were received by the insurance company P they were transferred as insurance premium under the general reinsurance contract in favour of insurance company X. By way of fictitious service contracts and commission payments made under an agency contract, insurance company X channelled the funds to several off-shore shell firms. Beneficiaries of the actual profit, being withdrawn abroad, were owners and directors of the construction company A.

FINANCING OF TERRORISM CASE STUDIES

Case study 1

In October a motor insurance policy was purchased by Mr X. The premium was based on 4 years no claims bonus and the premium was paid by way of debit/credit card via the internet. Mr X cancelled cover on the 5th November and asked for the refund of premium to be paid by personal cheque as he had lost the relevant debit/credit card.

On 3rd December Mr X contacted the insurer's call centre and took out cover on a different vehicle, a Vauxhall Corsa. This time he attempted to pay via a debit/credit card and initially the transaction was declined. The premium was paid in full by debit card the following day. Mr X now claimed that he had not earned any no claims bonus and bought every possible "added on" product. Once again Mr X requested that this policy be cancelled. He requested that the refund of premium should not be paid via the original debit card as that particular bank account had been closed. Consequently he asked for a personal cheque to be sent to him. This was refused with the insurer insisting that the refund should be paid via the original debit card. The insurer has subsequently established that the first refunded cheque was presented to cash converters.

Subsequent action

The series of transactions was reported to the FIU. Subsequent investigations indicated that the individual concerned appeared to be linked to a terrorist network.

Case study 2

An UK based insurer underwrote Jewellers block coverage for a Jewellery company based in Miami Florida, USA. A claim against the policy was made. However, the company owner, Mr X was unable to provide evidence of the loss and as a result an investigation took place. The investigation identified discrepancies in the financial records of the company and raised questions with regard to the movement of monies between bank accounts. Of significant interest was the transfer of funds to a bank account in Beirut. Under oath, Mr X stated that the account contained in excess of $200,000. No explanation for the movement of monies was provided and no bank statements were produced with regard to the bank account in the Middle East.

Subsequent action

This matter was reported to US law enforcement agencies by the insurer's attorneys. The law enforcement agencies were particularly interested in the movement of funds and indicated that these could have been used for the purposes of terrorist funding

Case study 3

A leader of a terrorist organisation instructed Mr X, who was trained in Afghanistan and fought U.S. forces in the country for several years, to set aside his initial intention to volunteer as a suicide bomber and sent him to Country A to support the organisation from there. In September 2004, Mr X attempted to acquire large sums of money from life insurance companies fraudulently, intending to direct a great part of this money to the terrorist organisation in order to fund its terrorist activities. To this end, Mr X recruited Mr Y and Mr Z, Mr Y's brother. Life insurance policies of 4 million euro were taken out for Mr Y with his brother, Mr Z, as the designated beneficiary. Mr Y was to fake a fatal traffic accident during his stay in Bountry B. By obtaining a death certificate, if necessary through bribery, the life insurance benefits were to be collected by Mr Z who would transfer the proceeds abroad via foreign bank accounts to fund terrorist activities. Mr X was primarily responsible for paying the insurance premiums for these life contracts. The plan was thwarted when Mr X and Mr Y were arrested in January 2005.

Subsequent action

Mr X and Mr Y were convicted of membership in a terrorist organisation and multiple counts of fraud. Mr X was sentenced to seven years in prison and Mr Y to six. Mr Z was also convicted of the lesser charge of supporting a terrorist organisation and fraud. He was sentenced to three and a half years in prison.