



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

Notice n^o 009/2008-AMCM

ASSUNTO: GUIDELINES ON PREVENTION AND COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM IN INSURANCE

Considering the need to revise the guidelines issued on prevention and combating money laundering and financing of terrorism in insurance;

Under the supervisory powers conferred on the AMCM by Articles 6 and 9 of its Charter, approved by Decree-Law No. 14/96/M, dated 11 March and pursuant to the terms of Article 10 paragraph 2 a) of Decree-Law No. 27/97/M, dated 30 June (Macao Insurance Ordinance), the Board of Directors of the AMCM hereby determines that:

- 1. In the prevention and combating money laundering and financing of terrorism, the insurance institutions and the insurance intermediaries shall comply with the guidelines contained in the document annexed to the present notice and which forms an integral part of this notice, as if the same were fully transcribed herein;*
- 2. Non-compliance with the guidelines on the part of the insurance institutions and the insurance intermediaries shall be punishable under the terms of the law applicable to the activity of insurance companies and insurance intermediaries, including the legal framework governing money laundering and financing of terrorism; and*
- 3. Notice No. 009/2006-AMCM, dated 18 August 2006 and Notice No. 012/2006-AMCM, dated 11 October 2006 are hereby revoked.*

Monetary Authority of Macao, 26 June 2008 – For and on behalf of the Board of Directors: Anselmo Teng, Chairman; António Félix Pontes, Executive Director



澳門金融管理局

AUTORIDADE MONETÁRIA DE MACAU

**GUIDELINES ON
PREVENTION AND COMBATING
MONEY LAUNDERING
AND FINANCING OF TERRORISM
IN INSURANCE**



Edition of
Monetary Authority of Macao
Insurance Supervision Department
(June 2008)

CONTENTS

	<i>Page</i>
<i>I. INTRODUCTION</i>	3
<i>II. BACKGROUND</i>	3
<i>II.1. What is money laundering and financing of terrorism?</i>	3
<i>II.2. Vulnerabilities in insurance</i>	3
<i>II.3. International initiatives</i>	4
<i>II.4. Stages of money laundering</i>	5
<i>II.5. Legislation on money laundering and on financing of terrorism in Macao</i>	6
<i>III. POLICIES, PROCEDURES AND CONTROLS TO BE ADOPTED BY INSURANCE INSTITUTIONS IN PREVENTION AND COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM</i>	7
<i>III.1. Customer acceptance</i>	8
<i>III.2. Customer due diligence (CDD)</i>	9
<i>III.2.1. General principle</i>	9
<i>III.2.2. Due diligence measures</i>	9
<i>III.2.3. Risk based approach to CDD</i>	10
<i>III.2.4. Simplified or reduced CDD measures</i>	11
<i>III.2.5. Complex, unusual large transactions or unusual patterns of transactions</i>	11
<i>III.2.6. Reinsurance business</i>	12
<i>III.2.7. Timing of identification and verification</i>	12
<i>III.2.8. Failure to satisfactorily complete CDD</i>	12
<i>III.2.9. Individuals</i>	12
<i>III.2.10. Corporations</i>	13
<i>III.2.11. Unincorporated businesses</i>	15
<i>III.2.12. Trust accounts</i>	15
<i>III.2.13. Higher risk customers</i>	16
<i>III.2.13.1. Customers of non-face-to-face transactions</i>	17
<i>III.2.13.2. Politically Exposed Persons (PEPs)</i>	18
<i>III.2.13.3. Non-Cooperative Countries and Territories (NCCTs)</i>	19
<i>III.2.14. On-going due diligence on existing customers and/or beneficial owners</i>	20
<i>III.2.15. Reliance on insurance intermediaries for customer due diligence</i>	21
<i>III.3. Record keeping</i>	21
<i>III.3.1. Requirements of the investigation and judicial authorities</i>	21
<i>III.3.2. Retention of records</i>	22
<i>III.4. Recognition and reporting of suspicious transactions</i>	23
<i>III.4.1. Recognition of suspicious transactions</i>	23
<i>III.4.1.1. Implementation of management information systems (MIS)</i>	23
<i>III.4.1.2. Identification of complex, unusual large transactions or unusual patterns of transactions</i>	23
<i>III.4.1.3. Regular customers/clients</i>	23
<i>III.4.1.4. Early encashments</i>	24
<i>III.4.1.5. Monitoring types of suspicious transactions</i>	24
<i>III.4.1.6. Guidelines in detecting financing of terrorism</i>	24

III.4.2. Reporting of suspicious transactions	25
III.4.2.1. Financial Intelligence Office (GIF)	25
III.4.2.2. Role and responsibilities of the Compliance Officer	25
III.5. Staff screening and training	26
III.5.1. Screening	26
III.5.2. The need for staff awareness	27
III.5.3. Training/Education packages	27
III.6. Compliance with law	28
III.7. Co-operation with law enforcement authorities	28
IV. GLOSSARY OF TERMS	30
V. ACRONYMS AND ABBREVIATIONS	33
VI. SOURCES OF THESE GUIDELINES	34
VII. ANNEXES	35
A. Indicators of suspicious transactions	35
B. Cases of money laundering and financing of terrorism in insurance business	38
C. List of recognized Stock Exchanges	40
D. Transactions linked to locations of concern (involving financial institutions)	41
E. Example for ratings for sensitive countries	42
F. Example for due diligence process	43
G. Example for approval process	43
H. Example for control process	44
I. Example for client risk rating	44
J. Sources of information	45
K. Report form to the Financial Intelligence Office	47

I. INTRODUCTION

1. *The increasing openness of the various economic systems provides different means of converting, transferring or dissimulating properties or proceeds derived from criminal activities, allowing perpetrators to utilise such properties or proceeds with impunity. To deal with this situation, international organisations are calling for solidarity of legislators and supervisory authorities in adopting adequate measures to prevent and repress such activities.*
2. *It is in this context that the AMCM has established the present Guidelines, which companies duly formed and authorised in Macao to carry on the business of insurance companies, private pension fund management companies, reinsurance companies, captive insurance companies and insurance intermediaries are obliged to follow in order to prevent and combat money laundering and financing of terrorism activities. In these Guidelines, the term “insurance institution(s)” refers not only to insurance company(ies), but also, with the necessary adaptations, to private pension fund management company(ies), reinsurance company(ies) and captive insurance company(ies).*

II. BACKGROUND

II.1. WHAT IS MONEY LAUNDERING AND FINANCING OF TERRORISM?

3. **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.*
4. *The main objective of money laundering would be to legitimise income originating from legal or illegal sources or businesses.*
5. **Financing of terrorism** *can be defined as the wilful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds should be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts. Terrorism can also be funded from legitimate income.*
6. *For terrorists, the acquisition of funds is not an end in itself but a means of committing a terrorist attack. With financing of terrorism, it does not matter whether the transmitted funds come from a legal or illegal source. Indeed, financing of terrorism frequently involves funds that, prior to being remitted, are unconnected to any illegal activity. Examples have occurred when legitimate funds have been donated to charities that, sometimes unknown to the donors, are actually fronts for terrorist organisations.*

II.2. VULNERABILITIES IN INSURANCE

7. *The insurance industry is vulnerable to money laundering and financing of terrorism. 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 before maturity or surrender, in order that payments can be made by the insurance institution 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.

8. *The most common form of money laundering or financing of terrorism that insurance institutions will encounter takes the form of a proposal to enter into a single premium contract. Examples of the type of contracts that are particularly attractive as a vehicle for laundering money or financing of terrorism are single premium investments e.g.:*
 - *Unit-linked or non unit-linked single premium contracts;*
 - *Purchased annuities;*
 - *Lump sum top-ups to an existing life contract; and*
 - *Lump sum contributions to personal pension contracts.*
9. *Money laundering or financing of terrorism in non-life insurance can be seen through inflated or totally bogus claims, e.g. by arson or other means causing a bogus claim to be made to recover part of the invested illegitimate funds. Examples of how the financing of terrorism could be facilitated through property and casualty coverage, include use of employee's compensation payments to support terrorists awaiting assignment and primary coverage and trade credit for the transport of terrorist materials.*
10. *Money laundering and the financing of terrorism using reinsurance could occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, fronting arrangements and captives or by the misuse of normal reinsurance transactions. Examples include:*
 - *The deliberate placement via the insurance institution of the proceeds of crime or terrorist funds with reinsurance companies in order to disguise the source of funds;*
 - *The establishment of bogus reinsurance companies, which may be used to launder the proceeds of crime or to facilitate terrorist funding; and*
 - *The establishment of bogus insurance institutions, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurance companies.*
11. *Insurance intermediaries are important for distribution, underwriting and claim settlement. They are often the direct link to the policyholder and, therefore, intermediaries should play an important role in the prevention and combating the money laundering and financing of terrorism.*
12. *The same principles that apply to insurance institutions should generally apply to insurance intermediaries. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of or does not conform to necessary procedures, or who fails to recognize or report information regarding possible cases of money laundering or financing of terrorism. The intermediaries themselves could have been set up to channel illegitimate funds to insurance institutions. In addition to the responsibility of intermediaries customer due diligence ultimately remains the responsibility of the insurance institution.*

II.3. INTERNATIONAL INITIATIVES

13. *The Financial Action Task Force on Money Laundering (FATF) was established in 1989 in an effort to thwart attempts by criminals to launder the proceeds of criminal activities*

through the financial system. Although Macao is not a member of FATF, it has participated regularly in the meetings organised by a similar entity at the regional level, as it is a member of the Asia/Pacific Group on Money Laundering (APG).

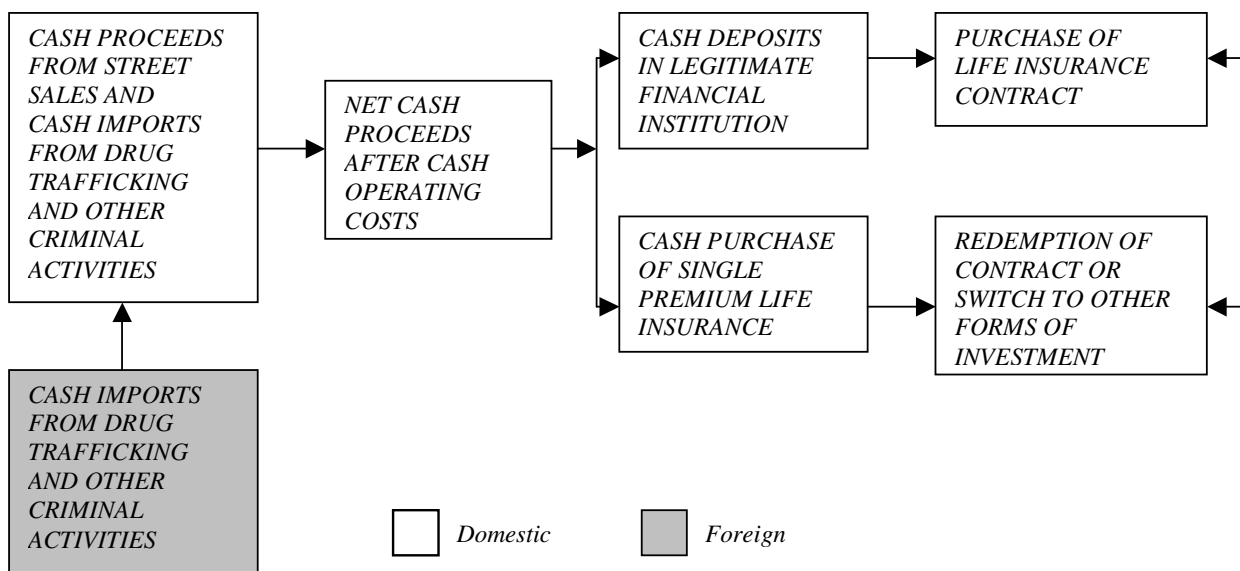
14. *The FATF has, among other things, put forward 40 Recommendations which cover the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation against money laundering. The latest version of 40 Recommendations was released in June 2003. In October 2001, the FATF expanded its scope of work to cover matters relating to financing of terrorism and promulgated Special Recommendations on Terrorist Financing (further updated in October 2004). These two sets of Recommendations, known as the 40+9 Recommendations, set out the international framework to detect, prevent and suppress money laundering and financing of terrorism activities. As a member of the APG, Macao is obliged to follow the measures in the Recommendations.*
15. *To keep in line with the development of prevention of money laundering and financing of terrorism standards in the financial sectors, the International Association of Insurance Supervisors (IAIS), in accordance with Insurance Core Principle (ICP) 28, issued a Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism in October 2004 which adapts the standards in the FATF 40+9 Recommendations to the specific practices and features of the insurance business. That Guidance Paper can be downloaded from IAIS's website at <http://www.iaisweb.org>.*

II.4. STAGES OF MONEY LAUNDERING

16. *There are three common stages of money laundering during which there may be numerous transactions made by the launderers that could alert an insurance institution to potential criminal activity:*
- **Placement** - *the physical disposal of cash proceeds derived from illegal activity;*
 - **Layering** - *separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity; and*
 - **Integration** - *creating the impression of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.*

17. *The following chart illustrates the laundering stages in more detail.*

LAUNDERING OF PROCEEDS



18. It is necessary to emphasize that insurance policies are mainly used by criminals in the first two stages (placement and layering) of the money-laundering process.

II.5. LEGISLATION ON MONEY LAUNDERING AND ON FINANCING OF TERRORISM IN MACAO

19. In order to address the problems associated with the laundering of proceeds from drug trafficking, the first initiative in the area of regulation in Macao was the enactment of a specific law - Decree-Law No. 5/91/M, of 28 January - with its Articles 22 and 34 providing for the freezing and confiscation of the proceeds and of the corresponding drugs and making the laundering of such proceeds a criminal offence. Nevertheless, the money-laundering crime as an autonomous illicit act on its own (that is to say, without being associated to the criminal activity generating the funds for laundering) was regulated in Macao only through Article 10 of Law No. 6/97/M, of 30 July.

20. More recently, the “Law on Prevention and Suppression of Money Laundering Crime” (Law No. 2/2006, of 23 March) and “Law on Prevention and Suppression of Terrorism Crimes” (Law No. 3/2006, of 30 March) have introduced substantial changes in the legislative structure of Macao by redefining respectively the types of money-laundering crimes and crimes associated with terrorism and terrorist activities (including the specific case of financing of terrorism) and by establishing a set of preventive measures that have to be followed for the prevention and combating of the said illicit activities. These preventive measures were subsequently concretised with regard to their specific content and scope of subjective application (that is, indicating which entities are required to comply with the said preventive measures) through Administrative Regulation No. 7/2006, of 7 April.

21. Among the preventive measures in the fight against money laundering and financing of terrorism activities, the said laws lay down the obligations of various economic operators to report to the Financial Intelligence Office (GIF) within two working days

from the date of execution of the operations suspected of involving conversion, transfer or dissimulation of illicit properties or proceeds.

22. *An important innovation introduced by Article 5 of the Administrative Regulation No. 7/2006, relates to the obligation to refuse the carrying out of the transactions on the part of the operators (insurance institutions and insurance intermediaries) whenever it is not possible to obtain the necessary client identification and transaction details.*
23. *Failure to comply with the above obligation is punishable with a fine of from MOP 10,000.00 (ten thousand patacas) to MOP 500,000.00 (five hundred thousand patacas) for an individual, or a fine of from MOP 100,000.00 (one hundred thousand patacas) to MOP 5,000,000.00 (five million patacas) for a corporate entity, pursuant to the terms of Article 9 of the Administrative Regulation No. 7/2006.*
24. *Similarly, supervisory authorities are required to inform immediately the Public Prosecutor's Office all cases of money laundering or financing of terrorism which have come to their knowledge in the course of their supervisory duties. They are also empowered to investigate cases of non-compliance with the reporting requirement and commence appropriate administrative infringement proceedings against entities under their supervision.*
25. *Article 3 of Law No. 2/2006 and Article 4 of Law No. 3/2006 make it a criminal offence to knowingly process or assist in the processing of illicit proceeds in order to disguise their illegal origin.*
26. *The maximum penalty applicable is a prison term of between 2 to 8 years in the case of money laundering or up to a maximum of 20 years in the case of crimes associated with terrorism and fine of up to 1,000 days or judicial liquidation when the crime is committed by a corporate entity.*
27. *On the other hand, a "tipping-off" offence is established in the Penal Code under which a person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigations including those relating to money laundering and financing of terrorism activities. The "tipping-off" offence carries a prison term of up to 1 year or alternatively a fine of up to 240 days.*

III. POLICIES, PROCEDURES AND CONTROLS TO BE ADOPTED BY INSURANCE INSTITUTIONS IN PREVENTION AND COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM

28. *The senior management of an insurance institution should be fully committed to establishing appropriate policies, procedures and controls for the prevention of money laundering and financing of terrorism and ensuring their effectiveness. Therefore the insurance institutions should have in place the following policies, procedures and controls:*
 - (a) *Insurance institutions should issue a clear statement of policies in relation to money laundering and financing of terrorism and communicate the policies to all management and relevant staff whether in branches, departments or subsidiaries and be reviewed on a regular basis;*

(b) Insurance institutions should develop instruction manuals setting out their procedures for:

- Customer acceptance;*
- Customer due diligence;*
- Record-keeping;*
- Recognition and reporting of suspicious transactions; and*
- Staff screening and training,*

based on the guidelines outlined respectively in the sections III.1., III.2., III.3., III.4., and III.5..

(c) Insurance institutions should instruct their internal audit/inspection departments to verify, on a regular basis, compliance with policies, procedures and controls against money laundering and financing of terrorism activities;

(d) Whilst appreciating the sensitive nature of extra-territorial regulations, and recognizing that their overseas operations must be conducted in accordance with local laws and regulations, insurance institutions should ensure that their overseas branches and subsidiaries are aware of the group policies concerning money laundering and financing of terrorism and, where appropriate, have been instructed to report to the local reporting point for their suspicious; and

(e) Insurance institutions should regularly review the policies, procedures and controls on money laundering and financing of terrorism to ensure their effectiveness.

III.1. CUSTOMER ACCEPTANCE

29. Prior to the establishment of a business relationship, insurance institutions should assess the characteristic of the required product, the purpose and nature of the business relationship and any other relevant factors in order to create and maintain a risk profile of the customer relationship. Based on this business risk assessment, the insurance institution should decide whether or not to accept the business relationship.

30. Insurance institutions should develop customer acceptance policies and procedures that aim to identify the types of customers (what is generally known as know your customer – KYC) and/or beneficial owners that are likely to pose a higher than average risk of money laundering and financing of terrorism. There should be clear internal guidelines on which level of management is able to approve a business relationship with such customers and/or beneficial owners. Decisions taken on establishing relationships with higher risk customers and/or beneficial owners should be taken by senior management.

31. In assessing the risk profile of a customer relationship, an insurance institution should consider the following factors:

- (a) Nature of the insurance policy, which is susceptible to money laundering risk, such as single premium policies;*
- (b) Frequency and scale of activities;*
- (c) Origin of the customer and/or beneficial owner (e.g. place of birth, residency), the place where the customer's and/or beneficial owner's business is established, the location of the counterparties with which the customer and/or beneficial owner*

conducts transactions and does business, such as Non-Cooperative Countries and Territories (NCCTs) designated by the FATF or named in the statement of concerns or other sanction lists with international implications (see III.2.13.3.), or those known to the insurance institution to be lack of proper standards in the prevention of money laundering;

- (d) Background or profile of the customer and/or beneficial owner, such as being, or linked to, a politically exposed person (see III.2.13.2.);*
 - (e) Nature of the customer's and/or beneficial owner's business, which may be particularly susceptible to money laundering risk, such as money changers or casinos that handle large amounts of cash;*
 - (f) Background or profile of the underlying principal where the customer is acting on behalf of another person;*
 - (g) For a corporate customer and/or beneficial owner, unduly complex structure of ownership for no good reason;*
 - (h) Means of payment as well as type of payment (cash, wire transfer, third party cheque without any apparent connection with the prospective customer and /or beneficial owner);*
 - (i) The source of funds / wealth; and*
 - (j) Any other information that may suggest that the customer and/or beneficial owner is of higher risk (e.g. knowledge that the customer and/or beneficial owner has been refused to enter a relationship by other financial institution).*
- 32. These are relevant factors that insurance institutions should consider in assessing the risk profile of their customers and/or beneficial owners. They, however, do not form part of the customer due diligence procedures (unless explicitly mentioned in these Guidelines).*
- 33. Following the initial acceptance of the customer and/or beneficial owner, a pattern of account activity that does not fit in with the insurance institution's knowledge of the customer and/or beneficial owner may lead the insurance institution to reclassify the customer and/or beneficial owner as higher risk.*

III.2. CUSTOMER DUE DILIGENCE (CDD)

III.2.1. General principle

- 34. Insurance institutions should make all the efforts to determine the true identity of all customers requesting their services. It should be an explicit policy that business transactions will not be conducted with customers who fail to provide evidence of their identities.*

III.2.2. Due diligence measures

- 35. Insurance institutions should not keep anonymous accounts or accounts in fictitious names. They should perform due diligence process for customers and/or beneficial owners. The measures should comprise the following:*

- (a) *Identify the customer and verify the customer's identity using reliable, independent source documents, data or information;*
 - (b) *Identify the beneficial owner and verify the identity of the beneficial owner such that the insurance institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, insurance institutions should understand their ownership and control structure;*
 - (c) *Obtain information on the purpose and intended nature of the business relationship between the customer and the insurance institution; and*
 - (d) *Conduct on-going due diligence and scrutiny, i.e. perform on-going scrutiny of the transactions and accounts throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the insurance institution's knowledge of the customers and/or beneficial owners, their businesses and risk profile, including, where necessary, identifying the source of funds.*
36. *If claims, commissions, and other monies are to be paid to persons or companies other than the customers or beneficial owners, then the proposed recipients of these monies should also be the subjects of identification and verification.*
37. *When an insurance institution or an insurance broker sends money to or receives money from its customers outside Macao (cross-border transfer) of MOP 20,000.00 (twenty thousand patacas) or above or an equivalent amount in any other currency, it should record the following particulars regarding the transaction:*
- (a) *Transaction serial number;*
 - (b) *Currency and amount involved;*
 - (c) *Date and time of receiving instructions from customers/instructors, if any;*
 - (d) *Instructions details (including method of delivery and receipt), if any;*
 - (e) *Name, identity card/passport number, telephone number and address of the customers/instructors;*
 - (f) *Bank accounts involved, if any; and*
 - (g) *Date and time of delivery and receipt, if any.*

III.2.3. Risk based approach to CDD

38. *The general rule is that customers and/or beneficial owners are subject to the full range of customer due diligence measures. Insurance institutions should however determine the extent of such measures on a risk based approach depending on the type of customer and/or beneficial owner, business relationship or transaction (factors for deciding the risk principle are set out in paragraph 31). Enhanced due diligence is called for with respect to higher risk categories. Conversely, it is acceptable for insurance institutions to apply simplified or reduced CDD measures for lower risk categories. Specific customer due diligence requirements applicable to certain types of customers are outlined in paragraphs 51 to 98.*
39. *The guiding principle of applying the risk based approach is that the insurance institutions should be able to justify that they have taken reasonable steps to satisfy*

themselves as to the true identity of their customers and/or beneficial owners. These measures should be objectively reasonable in the eyes of a third party. In particular, where an insurance institution is satisfied as to any matter it should be able to justify its assessment to the AMCM. Among other things, this would require the insurance institution to document its assessment and the reasons for it.

III.2.4. Simplified or reduced CDD measures

40. *In general, insurance institutions may apply simplified or reduced CDD measures in respect of a customer where there is no suspicion of money laundering and financing of terrorism, and*

- *The risk of money laundering and financing of terrorism is assessed to be low, for example, locally resident customers who have a business relationship which is understood by the insurance institutions; or*
- *There is adequate public disclosure in relation to the customers; or*
- *There are adequate checks and controls exist elsewhere in national systems.*

41. *Insurance institutions should bear in mind that the FATF lists the following examples of customers where simplified or reduced CDD measures could apply:*

- *Financial institutions – where they are subject to requirements to combat money laundering and the financing of terrorism consistent with the FATF Recommendations and are supervised for compliance with those controls;*
- *Public companies that are subject to regulatory disclosure requirements; or*
- *Government administrations or enterprises.*

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

- *Life insurance policies where the annual premium is no more than MOP8,000.00 (eight thousand patacas) or a single premium of no more than MOP20,000.00 (twenty thousand patacas), or an equivalent amount in any other currency;*
- *Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; or*
- *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 schemes.*

43. *Simplified or reduced CDD measures, however, are not acceptable whenever there is suspicion of money laundering or financing of terrorism or specific higher risk scenarios apply.*

III.2.5. Complex, unusual large transactions or unusual patterns of transactions

44. *Insurance institutions should pay special attention to all complex, unusual large transactions and all unusual patterns of transactions which have no apparent economic*

or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, and the findings should be established in writing. Insurance institutions are required to keep such findings available for competent authorities and auditors for at least five years. In this respect, “transactions” should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, premium payments, requests for changes in benefits, beneficiaries, duration, etc..

III.2.6. Reinsurance business

45. As to reinsurance, due to the nature of the business and the lack of a contractual relationship between the policyholder and the reinsurance company, it is often impractical for the reinsurance company to carry out verification of the policyholder and/or the beneficial owner. Therefore, for reinsurance business, reinsurance companies should only have business with ceding insurance institutions that are duly authorized and subject to the supervision by the AMCM or an equivalent authority in a jurisdiction that is a FATF member or that applies standards of prevention of money laundering and financing of terrorism equivalent to those of the FATF.

III.2.7. Timing of identification and verification

46. In principle, identification and verification of customers and beneficial owners should take place when the business relationship with those persons is established. This means that the customers and beneficial owners need to be identified and their identity verified before, or at the moment when, the insurance contract is concluded.

47. However, insurance institutions may permit the identification and verification of the beneficiary to take place after having established the business relationship, provided that the money laundering risks and financing of terrorism risks are effectively managed. In all such cases, identification and verification should occur before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

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

III.2.8. Failure of satisfactorily complete CDD

49. Where the insurance institution is unable to satisfy itself on the identity of the customer and/or beneficial owner, it should not commence business relationship or perform the transaction and should consider making a suspicious transaction report.

50. Where the insurance institution has already commenced the business relationship and is unable to satisfy itself on the identity of the customer and/or beneficial owner, it should consider terminating the business relationship, if possible, and making a suspicious transaction report.

III.2.9. Individuals

51. *Insurance institutions should institute effective procedures for obtaining satisfactory evidence of the identity of individual customers and/or beneficial owners including obtaining information about:*
- (a) True name and/or name(s) used (noted with documentary evidence);*
 - (b) Identity card/passport number;*
 - (c) Current permanent address;*
 - (d) Telephone number;*
 - (e) Date of birth;*
 - (f) Nationality (not mandatory when the individual is a holder of Macao Permanent Identity Card); and*
 - (g) Occupation/business (information about occupation/business is a relevant piece of information about a customer and/or beneficial owner but does not form part of the identification information requiring verification).*
52. *Identification documents such as current valid passports or identity cards should be produced as identity proof. For Macao residents, the prime source of identification will be the identity cards. File copies of identification documents should be retained.*
53. *In principle, copies of identification documents should be retained before, or at the moment when, the insurance contract is concluded. However, having considered the difficulty for insurance institutions to obtain copies of the identification documents when the sales process occurs outside the office, insurance institutions may obtain and keep copies of the identification documents after having established the business relationship provided that the money laundering risks and financing of terrorism risks are effectively managed. In all such circumstances, copies of identification documents should be obtained and copied for retention as soon as possible after the insurance contract is concluded and, in any cases, no later than the time of payout or the time when the beneficiary intends to exercise vested rights under the policy. Paragraph 48 provides guidance for adopting the risk management procedure.*
54. *It must be appreciated that no form of identification can be fully guaranteed as genuine or representing correct identity. If there is doubt about whether an identification document is genuine, contact should be made with Direcção dos Serviços de Identificação (Identification Department) or the relevant consulates in Macao to ascertain whether the details on the document are correct.*
55. *Insurance institutions should check the address of the applicant by appropriate means, e.g. by requesting sight of a recent utility or rates bill or a recent bank statement.*
56. *Insurance institutions should also identify the source of funds of customers and/or beneficial owners if the customers and/or beneficial owners are assessed to be of higher risk based on the factors set out in paragraph 31.*

III.2.10. Corporations

57. *Insurance institutions are required to verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person.*

Insurance institutions should also verify the legal status of the legal person or legal arrangements, information concerning the customer's name, legal form, address, directors and provisions regulating the powers to bind the legal person or arrangement. Examples of information that should be obtained are stated in the following paragraph.

58. *The following documents or information should be obtained in respect of corporate customers and/or beneficial owners which are registered in Macao, not being financial institutions as mentioned in paragraph 61 (comparable document, preferably certified by qualified persons such as lawyers or accountants in the country of registration, should be obtained for those customers and/or beneficial owners which are not registered in Macao, not being financial institutions as mentioned in paragraph 61);*
- (a) Certificate of incorporation and business registration certificate;*
 - (b) Memorandum and articles of association (if insurance institution considers necessary having regard to the risk of the particular transaction);*
 - (c) Resolution of the board of directors to enter into insurance contracts or other evidence conferring authority to those persons who will operate the insurance policy as well as the identification information of those persons; and*
 - (d) A search of the file at Commercial Registry, if there is a suspicion about the legitimacy of the legal entity.*
59. *It will generally be sufficient for an insurance institution to adopt simplified or reduced CDD measures in respect of a corporate customer and/or beneficial owner by obtaining the documents specified in the preceding paragraph if the risk of money laundering and financing of terrorism is assessed to be low. Some examples of lower risk corporate customers and/or beneficial owner are:*
- (a) The company is assessed to be of lower risk based on the factors set out in paragraph 31;*
 - (b) The company is listed on a recognized stock exchange (see Annex C) (or is a subsidiary of such listed company);*
 - (c) The company is a state-owned enterprise in a non-NCCT jurisdiction or in a country/jurisdiction not named in the statement of concerns or other sanction lists with international implications;*
 - (d) The company acquires an insurance policy for pension schemes if there is no surrender clause and the policy cannot be used as collateral; or*
 - (e) The company acquires 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.*
60. *Where a listed company on a recognized stock exchange is effectively controlled by an individual or a small group of individuals, an insurance institution should consider whether it is necessary to verify the identity of such individual(s).*
61. *Where a corporate customer and/or beneficial owner is a financial institution which is authorized and supervised by the AMCM or an equivalent authority in a jurisdiction that is a FATF member or that applies standards of prevention of money laundering and financing of terrorism equivalent to those of the FATF, it will generally be sufficient for*

an insurance institution to verify that the institution is on the list of authorized (and supervised) financial institutions in the jurisdiction concerned. Evidence that any individual representing the institution has the necessary authority to do so should be sought and retained.

- 62. In relation to corporate customer and/or beneficial owner which does not fall into the description of paragraphs 59 and 61, an insurance institution should look behind the company to identify the beneficial owners and those who have control over the funds. This means that, in addition to obtaining the documents specified in paragraph 58, the insurance institution should verify the identity of all the principal shareholders (a person entitled to exercise or control the exercise of 10% or more of the voting right of a company), at least two directors (including the managing director) of the company and all authorized signatories designated to sign insurance contracts. In case of one-director companies, insurance institutions are only required to verify the identity of that director. The insurance institution should also identify the source of funds. Besides, a search of the file in Commercial Registry should be performed.*
- 63. Where a corporate customer which does not fall into the descriptions of paragraphs 59 and 61; and which is a non-listed company and has a number of layers of companies in its ownership structure, the insurance institution should follow the chain of ownership to the individuals who are the ultimate principal beneficial owners of the customer of the insurance institution and to verify the identity of these individuals. The insurance institution, however, is not required to check the details of each of the intermediate companies (including their directors) in the ownership chain.*
- 64. An insurance institution should exercise special care in initiating business transactions with companies that have nominee shareholders. Satisfactory evidence of the identity of beneficial owners of such companies should be obtained.*
- 65. An insurance institution should also exercise special care in dealing with companies which have a significant proportion of capital in the form of bearer shares. The insurance institution should have procedures to monitor the identity of all principal shareholders. This may require the insurance institution to consider whether to immobilize the shares, such as by holding the bearer shares in custody.*
- 66. Where it is not practical to immobilize the bearer shares, insurance institutions should obtain a declaration from each owner (i.e. who holds 5% or more of the total shares) of the corporate customer on the percentage of shareholding. Such owners should also provide a further declaration on annual basis and notify the insurance institution immediately if the shares are sold, assigned or transferred.*

III.2.11. Unincorporated businesses

- 67. In the case of partnerships and other unincorporated businesses whose partners are not known to the insurance institution, satisfactory evidence should be obtained of the identity of at least two partners and all authorized signatories designated to sign insurance contracts in line with the requirements for individual applicants in paragraphs 51 to 56. In cases where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.*

III.2.12. Trust accounts

68. *Where trusts or similar arrangements are used, particular care should be taken in understanding the substance and form of the entity. Where the customer is a trust, the insurance institution should verify the identity of the trustees, any other person exercising effective control over the trust property, the settlers and the beneficiaries. Verification of the beneficiaries should be carried out prior to any payments being made to them.*
69. *When the verification of the identity of the settler is not possible, insurance institutions may accept a declaration from the trustee or other contractual party to confirm the link or relationship with the settler.*
70. *Insurance institutions should try as far as possible to obtain information about the identity of beneficiaries. A broad description of the beneficiaries such as family members of an individual may be accepted. Where the identity of beneficiaries has not previously been verified, insurance institutions should assess the need to undertake verification when they become aware that any payment out of the trust account is made to the beneficiaries or on their behalf. In making this assessment, insurance institutions should adopt a risk based approach which should take into account the amount(s) involved and any suspicion of money laundering or financing of terrorism. A decision not to undertake verification should be approved by senior management.*
71. *As with other types of customers, an insurance institution should adopt a risk based approach in relation to trusts and the persons connected with them. The extent of the due diligence process should therefore depend on factors such as the nature and complexity of the trust arrangement.*

III.2.13. Higher risk customers

72. *Insurance institutions should apply an enhanced due diligence in respect of higher risk customers and/or beneficial owners. Some examples of higher risk customers and/or beneficial owners are:*
- *Customers and/or beneficial owners are assessed to be of higher risk;*
 - *Customers of non-face-to-face transactions;*
 - *Policies/transactions with customers and/or beneficial owners where the annual insurance premium is MOP120,000.00 (one hundred and twenty thousand patacas) or above or an equivalent amount in any other currency. This includes situations where the insurance premium refers to one insurance policy/transaction or to several insurance policies/transactions that appear to be linked;*
 - *Politically exposed persons;*
 - *Non-resident customers;*
 - *Legal persons or arrangements, e.g. trust;*
 - *Companies with nominee shareholders; or*
 - *Customers in connection with NCCTs or with countries/jurisdictions named in the statement of concerns or other sanction lists with international implications.*
73. *Examples of additional measures applicable to enhanced due diligence are:*
- *Obtaining senior management approval for establishing business relationship;*

- *Obtaining comprehensive customer profile information e.g. purpose and reasons for entering the insurance contract, business or employment background, source of funds and wealth;*
- *Assigning a designated staff to serve the customer who bears the responsibility for customer due diligence and ongoing monitoring to identify any unusual or suspicious transactions on a timely basis;*
- *Requisition of additional documents to complement those which are otherwise required; and*
- *Certification by appropriate authorities and professionals of documents presented.*

74. Apart from the above general additional measures, specific additional measures are also applicable to the customers of non-face-to-face transactions (paragraphs 75 to 79); customers who are classified as politically exposed persons (paragraphs 80 to 86); and customers in connection with NCCTs (paragraphs 87 to 94) .

III.2.13.1. Customers of non-face-to-face transactions

- 75. An insurance institution should whenever possible conduct a face-to-face interview with a new customer to ascertain the latter's identity and background information, as part of the due diligence process. This can be performed either by the insurance institution itself or by an intermediary that can be relied upon to conduct proper customer due diligence.*
- 76. This is particularly important for higher risk customers. In this case, the insurance institution should ask the customer to make himself available for a face-to-face interview.*
- 77. New or developing technologies that might favour anonymity can be used to market insurance products. E-commerce or sales through internet or postal business is an example. Where face-to-face interview is not conducted, for example, where the account is opened via internet or post, an insurance institution should apply equally effective customer identification procedures and on-going monitoring standards as for face-to-face customers.*
- 78. Examples of specific measures that insurance institutions can use to mitigate the risk posed by such customers of non-face-to-face transactions include:*
- (a) Certification of identity documents presented by suitable certifiers;*
 - (b) Requisition of additional documents to complement those required for face-to-face customers;*
 - (c) Completion of on-line questionnaires for new applications that require a wide range of information capable of independent verification (such as confirmation with a government department);*
 - (d) Independent contact with the customer by the insurance institution;*
 - (e) Third party introduction through an intermediary which meets the criteria of customer due diligence.*
 - (f) Requiring the payment for insurance premiums through an account in the customer's name with a bank;*

- (g) *More frequent update of the information on customers of non-face-to-face transactions; or*
- (h) *In the extreme, refusal of business relationship without face-to-face contact for higher risk customers.*

79. *Insurance institutions are required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or financing of terrorism schemes.*

III.2.13.2. Politically Exposed Persons (PEPs)

80. *Business relationships with individuals holding important public positions as well as persons or companies clearly related to them (e.g. families, close associates, etc.) expose an insurance institution to particularly significant reputation or legal risks. There should be on-going enhanced due diligence in respect of such PEPs.*

81. *PEPs are defined as “Individuals who are or have been entrusted with prominent public functions in a foreign country, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials”. This definition does not cover middle ranking or more junior individuals in the foregoing categories and is equally applicable to family members and close associates of PEPs. The concern is that there is a possibility, especially in jurisdictions where corruption is widespread, that such PEPs may abuse their public powers for their own illicit enrichment through the receipt of bribes, etc..*

82. *An insurance institution should gather sufficient information from a new customer, and check publicly available information to establish whether or not the customer is a PEP. An insurance institution considering to establish a relationship with a person suspected to be a PEP should identify that person fully, as well as people and companies that are clearly related to him.*

83. *An insurance institution should also ascertain the source of funds before accepting a PEP as customer. The decision to establish business relationship with a PEP should be taken at a senior management level.*

84. *Risk factors that an insurance institution should consider in handling a business relationship (or potential relationship) with a PEP include:*

- (a) *Any particular concern over the jurisdiction where the PEP is from, taking into account his position;*
- (b) *Any unexplained sources of wealth or income (e.g. value of assets owned not in line with the PEP’s income level);*
- (c) *Unexpected receipts of large sums from governmental bodies or state-owned entities;*
- (d) *Source of wealth described as commission earned on government contracts;*
- (e) *Request by the PEP to associate any form of secrecy with a transaction; and*
- (f) *Use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.*

85. *Insurance institutions should determine and document their own criteria (including making reference to publicly available information or commercially available databases) to identify PEPs. A risk based approach may be adopted for identifying PEPs and focus may be put on persons from jurisdictions that are higher risk from a corruption point of view (reference can be made to publicly available information such as the **Corruption Perceptions Index**).*
86. *While paragraph 81 defines PEPs as individuals who hold prominent public functions outside Macao, insurance institutions are encouraged to extend the relevant requirements on PEPs to individuals who hold prominent public functions in Macao.*

III.2.13.3. Non-Cooperative Countries and Territories (NCCTs)

87. *The FATF has since the year 2000 engaged in a process of identifying countries and territories which have inadequate rules and practices that impede international cooperation in the fight against money laundering. Such countries/territories are designated as NCCTs or named in the statement of concerns.*
88. *The list of NCCTs or statement of concerns is published on the FATF website (<http://www.fatf-gafi.org>). The FATF reviews periodically the progress of these jurisdictions in addressing the deficiencies identified during the evaluation process.*
89. *An insurance institution should apply Recommendation 21 of the revised FATF Forty Recommendations to NCCTs and countries/jurisdictions named in the statement of concerns. This states that:*
- “Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities.”*
90. *Extra care should therefore be exercised by an insurance institution in respect of customers (including beneficial owners) from NCCTs or countries/jurisdictions named in the statement of concerns or other sanction lists with international implications. The business rationale for taking out the insurance policy should be clearly ascertained and should be properly documented. In addition, an insurance institution should be fully satisfied with the legitimacy of the source of funds of such customers.*
91. *For NCCTs, or countries/jurisdictions named in the statement of concerns, with serious deficiencies and where inadequate progress has been made to improve their position, the FATF may recommend the application of further counter-measures, which will generally focus on more stringent CDD and enhanced surveillance/reporting of transactions. An insurance institution should apply those counter-measures to such NCCTs or countries/jurisdictions named in the statement of concerns.*
92. *An insurance institution should be aware of the potential reputation risk of conducting business in NCCTs or countries/jurisdictions named in the statement of concerns or other jurisdictions known to apply inferior standards for the prevention of money laundering.*

93. *Insurance institutions are required to ensure that their overseas branches and subsidiaries observe AML/CFT measures consistent with Macao's requirements and the FATF's Recommendations, to the extent that local (i.e. host country) laws and regulations permit. Special attention should be given with respect to their branches and subsidiaries in countries which do not or insufficiently apply the FATF's Recommendations. If the minimum AML/CFT requirements of Macao and host countries differs, branches and subsidiaries in host countries should be required to apply the higher standard, to the extent that the host country laws and regulations permit.*
94. *Insurance institutions are required to inform the AMCM when an overseas branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by the host country laws, regulations or other measures.*

III.2.14. On-going due diligence on existing customers and/or beneficial owners

95. *Insurance institutions should perform on-going due diligence on the business relationship. In general, the insurance institutions should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. They should assess if the change/transaction does not fit the profile of the customer and/or beneficial owner or is for some other reason unusual or suspicious. Enhanced due diligence is required with respect to higher risk categories. The customer due diligence program should be established in such a way that insurance institutions are able to adequately gather and analyze information.*
96. *Examples of transactions or trigger events after establishment of the contract that require customer due diligence are:*
- (a) There is change in beneficiaries (for instance, to include non-family members, request for payments to persons other than beneficiaries);*
 - (b) There is significant increase in the amount of sum insured or premium payment that appears unusual in the light of the income of the policyholder;*
 - (c) There is use of cash and/or payment of large single premiums;*
 - (d) There is payment/surrender by a wire transfer from/to foreign parties;*
 - (e) There is payment by banking instruments which allow anonymity of the transaction;*
 - (f) There is change of address and/or place of residence of the policyholder and/or beneficial owner;*
 - (g) There are lump sum top-ups to an existing life insurance contract;*
 - (h) There are lump sum contributions to personal pension contracts;*
 - (i) There are requests for prepayment of benefits;*
 - (j) There is 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);*
 - (k) There is change of the type of benefit (for instance, change of type of payment from an annuity into a lump sum payment);*

- (l) *There is early surrender of the policy or change of the duration (where this causes penalties or loss of tax relief);*
 - (m) *There is request for payment of benefits at the maturity date;*
 - (n) *The insurance institution is aware that it lacks sufficient information about the customer and/or beneficial owner; or*
 - (o) *There is suspicion of money laundering and financing of terrorism.*
97. *Occurrence of these transactions and events does not imply that (full) customer due diligence needs to be applied. If identification and verification have already been performed, the insurance institution is entitled to rely on this unless doubts arise about the veracity of that information it holds. As an example, doubts might arise if benefits from one insurance policy are used to fund the premium payments of the insurance policy of another unrelated person.*
98. *Even when there is no specific trigger event, an insurance institution should consider whether to require additional information in line with current standards from those existing customers and/or beneficial owners that are considered to be of higher risk. In doing so, the insurance institution should take into account the factors mentioned in paragraph 31.*

III.2.15. Reliance on insurance intermediaries for customer due diligence

99. *An insurance institution may rely on insurance intermediaries to perform customer due diligence procedures. However, the ultimate responsibility of knowing the customer and/or beneficial owner always remains with the insurance institution. The insurance institution therefore should satisfy itself as to the adequacy of customer due diligence procedures conducted by the insurance intermediaries.*
100. *When such reliance is permitted, the insurance institution should immediately obtain the necessary information concerning the relevant identification data and other documentation relating to CDD requirements pertaining to the identity of the customer and/or beneficial owner from the insurance intermediary. The insurance intermediary should submit such information to the insurance institution upon request without delay.*
101. *The purpose of obtaining the underlying documentation is to ensure that it is immediately available on file for reference purposes by the insurance institution or relevant authorities such as the AMCM and the GIF, and for on-going monitoring of the customer and/or beneficial owner. It will also enable the insurance institution to verify that the insurance intermediary is doing its job properly. It is not the intention that the insurance institution should use the documentation, as a matter of course, to repeat the due diligence conducted by the insurance intermediary.*
102. *The insurance institution should undertake and complete its own verification of the customer and beneficial owner if it has any doubts about the ability of the insurance intermediary to undertake appropriate due diligence.*

III.3. RECORD KEEPING

III.3.1. Requirements of the investigation and judicial authorities

103. *The Penal Code and the Penal Procedures Code entitle the Judiciary Police and the Court to examine all relevant past transactions to assess whether the defendant has benefited from drug trafficking or other indictable offences. Records should be available to domestic competent authorities upon appropriate authority.*
104. *The investigating authorities need to ensure a satisfactory audit trail for suspected drug related or other laundered money or financing of terrorism and to be able to establish a financial profile of the suspect account.*
105. *An important objective of record keeping is to ensure that insurance institutions can, at all stages in a transaction, retrieve relevant information to the extent that it is available without undue delay.*

III.3.2. Retention of records

106. *Insurance institutions should keep records on the risk profile of each customer and/or beneficial owner and the data obtained through the CDD process (e.g. name, address, the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction), the copies of official identification documents (such as passports, identity cards or similar documents) and the account files and business correspondence, for at least 5 years after the end of the business relationship, or longer, if requested by a competent authority in specific cases and upon proper authority.*
107. *Insurance institutions should maintain, for at least 5 years (or longer, if requested by a competent authority in specific cases and upon proper authority) after the business relationship has ended, all necessary records on transactions, both domestic and international, and be able to respond to the information request from the competent authorities in a timely manner. Such records must be sufficient to permit reconstruction of individual transactions (including the amount and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.*
108. *Insurance institutions should ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of clients or business relationships.*
109. *Insurance institutions should ensure that they have in place adequate procedures:*
- (a) To access initial proposal documentation including, where these are completed, the client financial assessment, client needs analysis, copies of regulatory documentation, details of the payment method, illustration of benefits, and copies of documentation in support of verification by the insurance institution;*
 - (b) To access all post-sale records associated with the maintenance of the contract, up to and including maturity of the contract; and*
 - (c) To access details of the maturity processing and/or claim settlement including completed “discharge documentation”.*
110. *Retention may be by way of original documents, stored on microfiche, or in computerised form provided that such forms are accepted as evidence. In situation where*

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

III.4. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

III.4.1. Recognition of suspicious transactions

III.4.1.1. Implementation of management information systems (MIS)

111. In order to satisfy an insurance institution's legal and regulatory obligations, it needs to have systems to enable it to identify and report suspicious transactions. However, it is not enough to rely simply on the initiative of front-line staff to make ad hoc reports. An insurance institution should also have management information systems (MIS) to provide managers and compliance officers with timely information on a regular basis to enable them to detect patterns of unusual or suspicious activity, particularly in relation to higher risk accounts.

112. This also requires the insurance institution to have a good understanding of what is normal and reasonable activity for particular types of customer and/or beneficial owner, taking into account the nature of its business. Among other things, an insurance institution should take appropriate measures to satisfy itself about the source and legitimacy of funds to be credited to a customer's and/or beneficial owner's account. This is particularly the case where large amounts are involved.

III.4.1.2. Identification of complex, unusual large transaction or unusual patterns of transactions

113. MIS reports used for monitoring purposes should be capable of identifying transactions that are unusual either in terms of amount (for example, by reference to predetermined limits for the customer in question or to comparative figures for similar customers) or type of transaction or other relevant risk factors.

114. To facilitate the identification of suspicious transactions, indicators of suspicious transactions are given in Annex A and examples of money laundering schemes involving insurance are given in Annex B. The indicators are not intended to be exhaustive and are for reference only. Identification of any of the types of transactions listed in Annex A should prompt further investigation and be a catalyst towards making at least initial enquiries about the source of funds.

III.4.1.3. Regular customer/clients

115. As the types of transactions used for money laundering or financing of terrorism are almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of policyholder. Therefore, the first key to recognition is knowing enough about the customer's business to recognise that a transaction, or series of transactions, is unusual.

III.4.1.4. Early encashments

116. *Requests for early encashment of single premium policies, particularly for cash or settlement to an individual third party, could be regarded as grounds for suspicion in that such activity may be used as part of the layering process for money laundering or financing of terrorism purposes. Early encashments are generally regarded as those taking place within 2 years of contract date.*

III.4.1.5. Monitoring types of suspicious transactions

117. *The list of examples of suspicious transactions needs to be continually overseen by a senior officer responsible for ensuring day-to-day consideration of money laundering or financing of terrorism techniques. Each insurance institution should formally designate an officer to be responsible for money laundering deterrence and reporting procedures. That officer should be in a position to provide advice on suspicious transactions both internally and to the law enforcement agencies.*

III.4.1.6. Guidelines in detecting financing of terrorism

118. *In relation to financing of terrorism, the FATF issued in April 2002 a Guidance for Financial Institutions in Detecting Terrorist Financing. The document describes the general characteristics of financing of terrorism with case studies illustrating the manner in which law enforcement agencies were able to establish a financing of terrorism link base on information reported by financial institutions. One of these annexes of that document contains a series of characteristics of financial transactions that have been linked to terrorist activity in the past (see Annex D). An insurance institution should acquaint itself with the FATF paper.*

119. *An insurance institution should maintain a database of names and particulars of terrorist suspects which consolidates the various lists that have been made known to it. Alternatively, an insurance institution may make arrangements to secure access to such a database maintained by third party service providers.*

120. *Such database should include the lists and measures under the international conventions signed and ratified by the Central Government applicable to Macao Special Administrative Region (Macao SAR). Under Law No.4/2002 of 15 April (“Law Relating to the Fulfilment of Certain Acts of International Laws”), the anti-terrorism measures under Resolution No.1373 and other relevant resolutions of the United Nation Security Council become applicable to Macao SAR. The lists of individuals/entities designated as terrorists shall be published in the Official Gazette from time to time. As such, the database should also be subject to timely update whenever there are changes, and should be made easily accessible by staff for the purpose of identifying suspicious transactions.*

121. *An insurance institution should check the name of both existing customers and/or beneficial owners as well as new applicants for business against the names in the database. It should be particularly alert for suspicious remittances and should bear in mind the role which non-profit organizations are known to have played in financing of terrorism. Enhanced checks should be conducted before processing a transaction, where possible, if there are circumstances giving rise to suspicion.*

III.4.2. Reporting of suspicious transactions

III.4.2.1. Financial Intelligence Office (GIF)

122. *The reception point for disclosures of any suspicious transaction (STR-Suspicious Transaction Report) under the relevant laws is the Financial Intelligence Office (GIF) set up by the Dispatch No. 227/2006 of the Chief Executive, of 29 July.*
123. *In addition to acting as the point for receipt of disclosures made by an organization or individual, the GIF also acts as domestic and international advisor on money laundering and financing of terrorism generally and offers practical guidance and assistance to the financial sector (among others) on those matters.*

III.4.2.2. Role and responsibilities of the Compliance Officer

124. *The obligation to report is on the individual who becomes suspicious of money laundering or financing of terrorism transaction. Each insurance institution should appoint a designated officer or officers (“**Compliance Officer(s)**”) at the management level who should be responsible for reporting to the GIF where necessary in accordance with the relevant legislation and to whom all internal reports should be made.*
125. *The role and responsibilities of the compliance officer should not be simply that of a passive recipient of ad hoc reports of suspicious transactions. Rather, the compliance officer should play an active role in the identification and reporting of suspicious transactions. The compliance officer and the appropriate staff should have timely access to customer identification data, and other CDD information, transaction records and other relevant information. This should involve regular review of exception reports of large or irregular transactions generated by the insurance institution’s MIS as well as ad hoc reports made by front-line staff. Depending on the organization structure of the insurance institutions, the specific task of reviewing reports may be delegated to other staff but the compliance officer should maintain oversight of the review process.*
126. *All cases, where an employee suspects or has reasonable grounds to believe that a customer might have carried on drug trafficking or might have been engaged in other indictable offences and where the customer seeks to take out, maintain or redeem a policy with the insurance institution, must promptly be reported to the compliance officer. The compliance officer must promptly evaluate whether there are reasonable grounds for such belief and must then immediately report the case to the GIF, unless he considers, and records his opinion, that such reasonable grounds do not exist.*
127. *The compliance officer should form a considered view on whether unusual or suspicious transactions should be promptly reported to the GIF. In reporting to the GIF, the compliance officer should ensure that all relevant details are provided in the report and cooperate fully with the GIF for data collection purposes. If a decision is made not to report an apparently suspicious transaction to the GIF, the reasons for this should be fully documented by the compliance officer. The fact that a report may already have been filed with the GIF in relation to previous transactions of the customer and/or beneficial owner in question should not necessarily preclude the making of a fresh report if new suspicions are aroused.*
128. *The compliance officer should keep a register of all reports made to the GIF and all reports made to them by employees. The compliance officer should provide employees*

with a written acknowledgement of reports made to them, which will form part of the evidence that these reports were made in compliance with the internal procedures.

129. The compliance officer should have the responsibility for checking on an ongoing basis that the insurance institution has policies and procedures to ensure compliance with legal and regulatory requirements and of testing such compliance.

130. It follows from this that the insurance institution should ensure that the compliance officer is of sufficient status within the organization and has adequate resources, to enable him to perform his functions.

131. If an insurance agent or insurance broker who considers funds offered in settlement of a contract to be suspicious will share that suspicion with his insurance institution, in addition to reporting it directly to the GIF. He could inform his insurance institution either at the time when the disclosure is made to the GIF or when the documentation is passed to the insurance institution for processing.

132. Insurance institutions are required to maintain an adequately resourced and independent audit function to test compliance (including sample testing) on a periodic basis with internal procedures, policies and controls to prevent money laundering and financing of terrorism. The internal audit function should include, but not limited to, checking the effectiveness of the compliance function, the adequacy of MIS reports of large or irregular transactions and the quality of reporting of suspicious transactions. The level of awareness of front line staff of their responsibilities in relation on the prevention of money laundering and financing of terrorism should also be reviewed. As in the case of the compliance officer, the internal audit function should have sufficient expertise and resources to enable it to carry out its responsibilities. It is of importance that the auditor has direct access and reports directly to the management and the board of directors.

133. Insurance institutions are required to report all suspicious transactions, including attempted transactions, within two working days to the GIF using the standard form attached to these guidelines (see Annex K). Explanatory notes on the procedures and the method of filing suspicious transaction reports are contained in the report form.

III.5. STAFF SCREENING AND TRAINING

III.5.1. Screening

134. Insurance institutions should identify the key positions within their organizations with respect to anti-money laundering and combat of financing of terrorism and should develop the following internal procedures for assessing whether employees taking up the key positions meet fit and proper requirements and are of high standards:

- (a) Verification of the identity of the person involved;*
- (b) Verification of the certificate of no criminal record of the person involved; and*
- (c) Verification whether the information and references provided by the employee are correct and complete.*

135. *Insurance institutions should keep records on the identification data obtained from their employees mentioned in the preceding paragraph. The records should demonstrate the due diligence performed in relation to the fit and proper requirements.*

III.5.2. The need for staff awareness

136. *Staff must be aware of their own personal obligations under the Penal Code and the specific laws about money laundering and financing of terrorism and that they can be personally liable for failing to report information to the authorities. They are advised to read the relevant sections of such regulations. They must be encouraged to co-operate fully with the law enforcement agency and to provide prompt notice of suspicious transactions. They should be advised to report suspicious transactions to their institution's Compliance Officer(s) if they do not know precisely what the underlying criminal activity is or whether illegal activities have occurred.*

137. *It is, therefore, imperative that insurance institutions introduce comprehensive measures to ensure that staff are fully aware of their responsibilities.*

III.5.3. Training/Education packages

138. *Insurance institutions are required to establish ongoing training to employees and intermediaries to ensure that they are kept informed of new developments, including information on current money laundering and financing of terrorism techniques, methods and trends. The training should include all aspects of AML/CFT laws and obligations, and, in particular, requirements concerning CDD and suspicious transaction reporting. Timing and content of training packages for various sectors of staff/intermediaries need to be adapted by individual institutions for their own needs. Other than the above-mentioned areas, the training program should also include the following:*

(a) New employees

A general appreciation of the background to money laundering and financing of terrorism, and the subsequent need for identifying and reporting of any suspicious transactions to the appropriate designated point, should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicious transactions by the insurance institution, that there is a legal requirement to report, and that there is a personal statutory obligation in this respect.

(b) Sales/Advisory staff

Members of staff who are dealing directly with the public (whether as members of staff, agents or salesmen) are the first point of contact with potential money launderers or financiers of terrorists and their efforts are therefore vital to the strategy in the fight against money laundering and financing of terrorism. They should be made aware of their legal responsibilities, including the insurance institution's reporting system for such transactions. Training should be provided on areas that may give rise to suspicious transactions and on the procedures to be adopted when a transaction is deemed to be suspicious. It is that "front-line" staffs are made aware of the insurance institution's policy for dealing in certain

circumstances particularly where large transactions are involved, and the need for extra vigilance in these cases.

(c) Processing staff

Those members of staff who receive completed proposals and cheques for payment of the single premium contribution must receive appropriate training in the processing and verification procedures. The identification of the proponent and the matching against the cheque received in settlement are, for instance, key processes. Such staff should be aware that the offer of suspicious funds accompanying a request to undertake an insurance contract may need to be reported to the relevant authorities irrespective of whether or not the funds are accepted or the proposal proceeded with. Staff must know what procedures to follow.

(d) Administration/Operations supervisors and managers

A higher level of instruction covering all aspects of money laundering or financing of terrorism procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the Penal Code and the specific laws about money laundering and financing of terrorism; procedures relating to service of production and restraint orders; and the requirements for retention of records.

(e) Compliance officers

The compliance officer should receive in-depth training concerning all aspects of relevant legislation, guidelines and policies and procedures on the prevention of money laundering and financing of terrorism.

(f) Ongoing training

It will also be necessary to make arrangements for refresher training at regular intervals to ensure that staff do not forget their responsibilities. It is suggested that this might be best achieved by a twelve or six-monthly review of training or, alternatively, a review of the instructions for recognising and reporting suspected money laundering or financing of terrorism transactions.

III.6. COMPLIANCE WITH LAW

139. Management of insurance institutions should ensure that business is conducted in conformity with high ethical standards and that laws and regulations pertaining to financial transactions are adhered to. As regards transactions executed on behalf of customers, it is accepted that insurance institutions may have no means of knowing whether the transaction stems from or forms part of criminal activity. Nevertheless, insurance institutions should not set out to offer services or provide active assistance in transactions which they have good reason to suppose are associated with money laundering or financing of terrorism activities.

III.7. CO-OPERATION WITH LAW ENFORCEMENT AUTHORITIES

140. Insurance institutions should co-operate fully with law enforcement authorities to the extent permitted by law or contractual obligations relating to customer confidentiality.

Care should be taken to avoid providing support or assistance to customers seeking to deceive law enforcement agencies through the provision of altered, incomplete or misleading information. Where insurance institutions become aware of facts which lead to the reasonable presumption that money used in purchasing single premium policies stems from criminal activities, appropriate measures, being consistent with the law and having regard to the contractual obligations of the insurance institutions concerned, should be taken, for example, to deny assistance, sever relations with the customer and freeze redemption of the policy contract.

IV. GLOSSARY OF TERMS

Attempted transactions – mean those where the insurance institution has not completed the transactions or customer due diligence, regardless of whether the business relationship has established or not.

Beneficiary – is the recipient of the insurance institution's benefit.

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

Business relationship – means a continuing arrangement between the insurance institution in question and another party, to facilitate the carrying out of transactions, in the course of such insurance business – (i) on a frequent, habitual, or regular basis; and (ii) where the monetary value of any transactions to be carried out in the course of the arrangement is not known on entering into the arrangement.

Business risk assessment – is an assessment which documents the exposure of a business to money laundering and financing of terrorism risks and vulnerabilities taking into account its size, nature and complexity and its customers, products and services and the way in which it provides those services.

Captive insurance company – is a limited-purpose, wholly owned, insurance subsidiary of an organization not in the insurance business, which has as its primary function the insuring of some of the exposures and risks of its parent or the parent's affiliates.

Compliance Officer – is the designated officer at the management level who should be responsible for reporting to the GIF where necessary in accordance with the relevant legislation and to whom all internal reports should be made.

Cross-border transfer – means to any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfer that has at least one cross-border element.

Currency – refers to banknotes and coins that are in circulation as a medium of exchange.

Customer – refers to the policyholder.

Customer due diligence (CDD) – are the steps which an insurance institution is required to carry out in order to identify and verify the identity of the parties to a relationship and to obtain information on the purpose and intended nature of each business relationship.

Customer due diligence information – encompasses identification data and any files and correspondence relating to the business relationship.

Document – includes information recorded in any form (including without limitation, in electronic form).

Employee – is an individual working, including on a temporary basis, for an insurance institution whether a contract of employment, a contract for services or otherwise.

FATF Recommendations – refers to the Forty Recommendations and the Nine Special Recommendations on Financial of Terrorism issued by the FATF. Those (40+9) Recommendations can be downloaded from FATF website at <http://www.fatf-gafi.org>.

Funds – are assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable and legal documents or instruments evidencing title to, or interest in, such assets.

Identification data – means data, documents, in any form whatsoever, which is from a reliable and independent source.

Insured – is the natural or legal person in whose interest the contract is agreed, or the person whose life, health or physical integrity is insured.

Insurance company – includes an insurance company incorporated in Macao or a branch of an overseas insurance company.

Insurance institution(s) – includes insurance company(ies), private pension fund management company(ies), reinsurance company(ies) and captive insurance company(ies).

Insurance intermediaries – include insurance agents (individuals or corporations), insurance salesmen and insurance brokers.

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

Legal persons – refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with an insurance institution or otherwise own property.

Policyholder – is the natural or legal person who, on his own behalf or on behalf of one or several persons, enter into an insurance contract with the insurance institution and is responsible for the payment of the premium.

Private pension fund management company – includes a life insurance company or a company set up specifically to manage private pension funds.

Proceeds – refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.

Reinsurance company – includes a reinsurance company incorporated in Macao or a representative office of an overseas reinsurance company.

Risk – all references to **risk** in these guidelines refers to the risk of money laundering and/or financing of terrorism.

Transactions – should be understood to refer to the insurance product itself, the premium payment and the benefits; in other words, means inquiries and applications for an insurance policy, premium payments, requests for changes in benefits, beneficiaries, duration, etc..

V. **ACRONYMS AND ABBREVIATIONS**

The following acronyms and abbreviations refer to the full version of the following names:

AMCM – Monetary Authority of Macao

AML – Anti Money Laundering

APG – Asia/Pacific Group

CDD – Customer Due Diligence

CFT – Combating the Financing of Terrorism

CPI – Corruption Perceptions Index

ERG – Export Risk Guarantee

FATF – Financial Action Task Force on Money Laundering

FINCEN – Financial Crimes Enforcement Network

GAFI – Groupe d’Action Financière

GIF – Financial Intelligence Office

IAIS – International Association of Insurance Supervisors

ICP – Insurance Core Principle(s)

KYC – Know Your Customer

MIS – Management Information Systems

NCCTs – Non-Cooperative Countries and Territories

OFAC – Office of Foreign Assets Control

PEPs – Politically Exposed Persons

STR – Suspicious Transaction Report

TI – Transparency International

VI. SOURCES OF THESE GUIDELINES

- *Law No. 4/2002, of 15 April (Law Relating to the Fulfillment of Certain Acts of International Laws);*
- *Law No. 2/2006, of 23 March (Law on Prevention and Suppression of Money Laundering Crime);*
- *Law No. 3/2006, of 30 March (Law on Prevention and Suppression of Terrorist Crimes);*
- *Administrative Regulation No. 7/2006, of 7 April (Preventive measures against crimes of money laundering and of financing of terrorism);*
- *Dispatch No. 227/2006 of the Chief Executive, of 29 July (Setting up of Financial Intelligence Office);*
- *Money Laundering – A Guide for Insurance Institutions (U.S. Department of Justice – Federal Bureau of Investigation – March, 1993);*
- *Guidance for Financial Institutions in Detecting Terrorist Financing (Financial Action Task Force on Money Laundering – April, 2002)*
- *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism (International Association of Insurance Supervisors – October 2004);*
- *Guidance Note on Prevention of Money Laundering and Terrorist Financing (The Office of the Commissioner of Insurance of Hong Kong – July 2005);*
- *How to Combat Money Laundering and Terrorist Financing – The Regulator’s Guide (Edited by Richard Pratt – Central Banking Publications Ltd. – 2005); and*
- *Handbook for Financial Services Business on Countering Financial Crime and Terrorist Financing (Guernsey Financial Services Commission – September 2007).*

VII. ANNEXS**ANNEX A****INDICATORS OF SUSPICIOUS TRANSACTIONS****➤ MONEY LAUNDERING OR FINANCING OF TERRORISM USING SINGLE PREMIUM INSURANCE CONTRACTS**

- *A request by a client to enter into an insurance contract(s) where the source of the funds is unclear or not consistent with the customer's apparent standing;*
- *A sudden request for a significant purchase of a lump sum contract with an existing client whose current contracts are small and of regular payments only;*
- *A proposal which has no discernible purpose and a reluctance to divulge a "need" for making the investment;*
- *A proposal to purchase and settle by cash;*
- *A proposal to purchase by utilising a cheque drawn other than from the personal account of the proposer;*
- *The prospective client who does not wish to know about investment performance but does inquire on the early cancellation/surrender of the particular contract.*

➤ MONEY LAUNDERING OR FINANCING OF TERRORISM BY OFFSHORE INTERNATIONAL ACTIVITY

- *The customer who is introduced by an overseas agent, affiliate or other company that is based in NCCTs designated by the FATF from time to time or in countries where corruption or the production of drugs or drug trafficking may be prevalent;*
- *The customer who is based in Macao and is seeking a lump sum investment and offers to pay by a wire transaction or foreign currency.*

➤ MONEY LAUNDERING OF FINANCING OF TERRORISM INVOLVING INSURANCE INSTITUTION, EMPLOYEE AND AGENT

- *Unexpected changes in employee characteristics, e.g. lavish lifestyle or avoiding taking holidays;*
- *Unexpected change in employee or agent performance, e.g. the sales person selling products has a remarkable or unexpected increase in performance;*

- *Consistently high activity levels of single premium business far in excess of any average insurance institution expectation;*
- *The use of an address which is not the client's permanent address, e.g. utilisation of the salesman's office or home address for the dispatch of customer documentation.*

➤ **OTHER INDICATORS OF MONEY LAUNDERING USING INSURANCE CONTRACTS**

- *Early termination of a product, especially in a loss;*
- *A customer applies for an insurance policy relating to business outside the customer's normal pattern of business;*
- *A customer requests for a purchase of insurance policy in an amount considered to be beyond his apparent need;*
- *A customer attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments;*
- *A customer refuses, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue;*
- *A customer is reluctant to provide normal information when applying for an insurance policy, provides minimal or fictitious information or provides information that is difficult or expensive for the insurance institution to verify;*
- *Delay in the provision of information to unable verification to be completed;*
- *Opening accounts with the customer's address outside the local service area;*
- *Opening accounts with names similar to other established business entities;*
- *Attempting to open or operating accounts under a false name;*
- *Any transaction involving an undisclosed party;*
- *A transfer of the benefit of a product to an apparently unrelated third party;*
- *A change of the designated beneficiaries, especially if this can be achieved without knowledge or consent of the insurance institution and/or the right to payment could be transferred simply by signing an endorsement on the policy;*
- *Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policyholder;*
- *The customer accepts very unfavourable conditions unrelated to his health or age;*
- *An atypical incidence of pre-payment of insurance premiums;*

- *Insurance premiums have been paid in one currency and requests for claims to be paid in another currency;*
- *Activity is incommensurate with that expected from the customer considering the information already known about the customer and the customer's previous financial activity (For individual customers, consider customer's age, occupation, residential address, general appearance, type and level of previous financial activity. For corporate customers, consider type and level of activity);*
- *Any unusual employment of an intermediary in the course of some usual transaction or formal activity, e.g. payment of claims or high commission to an unusual intermediary;*
- *A customer appears to have policies with several insurance institutions;*
- *A customer wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.*

CASES OF MONEY LAUNDERING AND FINANCING OF TERRORISM IN INSURANCE BUSINESS

➤ **LIFE INSURANCE**

- *In 1990, a British insurance sales agent was convicted of violating a criminal money-laundering statute. The insurance agent was involved in a money-laundering scheme in which over USD1.5 million was initially placed with a bank in England. The “layering process” involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance institution and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent’s supervisor was also charged with violating the money-laundering statute. This case has shown how money laundering has reached into the insurance industry and if coupled with a corrupt employee can expose an insurance institution to negative publicity and possible criminal liability.*
- *On a smaller scale and more recently, local police authorities were investigating the placement of cash by a illegal drug trafficker. The funds were deposited into several bank accounts and then transferred to an offshore account. The drug trafficker then entered into a USD 75,000 life insurance policy. Payment for the policy was made by two separate wire-transfers from the offshore accounts. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker’s arrest, the insurance institution had received instructions for the early surrender of the policy.*
- *A customer contracted life insurance of a 10 year duration with a cash payment equivalent to around USD 400,000. Following payment, the customer refused to disclose the origin of the funds. The insurance institution reported the case. It appears that prosecution had been initiated in respect of the individual’s fraudulent management activity.*

➤ **NON-LIFE INSURANCE**

- *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 insurance institution 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 institution, and few questioned the source of the funds having seen the name of the company on the cheque or wire transfer.*

➤ **INTERMEDIARIES**

- *A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of USD250,000 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 institution branch. The insurance broker delivered, afterwards, to the insurance institution 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 institution.

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

➤ **REINSURANCE**

- *A state insurance institution in country A sought reinsurance cover for its cover of an airline company. When checking publicly available information on the company it turned out that the company was linked to potential warlords and drug traffickers. A report was made to the law enforcement authorities.*

➤ **CLAIMS**

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

➤ **FRAUDULENT CLAIMS AND FINANCING OF TERRORISM**

- *An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance institution then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organisation running the operation sells the motor vehicle and pockets the profit from its sales. In one instance, an insurance institution suffered losses in excess of USD2 million from similar fraud schemes carried out by terrorist groups.*

ANNEX C

LIST OF RECOGNIZED STOCK EXCHANGES

- *American Stock Exchange;*
- *Athens Stock Exchange;*
- *Australian Stock Exchange;*
- *Bursa Malaysia;*
- *Copenhagen Stock Exchange;*
- *Deutsche Borse AG;*
- *Euronext Amsterdam;*
- *Euronext Lisbon;*
- *Euronext Paris;*
- *Helsinki Stock Exchange;*
- *Hong Kong Exchange and Clearing Limited;*
- *Irish Stock Exchange;*
- *Italian Stock Exchange;*
- *Jasdaq Securities Exchange;*
- *Korea Exchange;*
- *London Stock Exchange;*
- *Luxembourg Stock Exchange;*
- *Madrid Stock Exchange;*
- *Mexican Stock Exchange;*
- *Nagoya Stock Exchange;*
- *NASDAQ;*
- *New York Stock Exchange;*
- *New Zealand Exchange;*
- *Osaka Securities Exchange;*
- *Oslo Bors;*
- *Pacific Exchange;*
- *Philadelphia Stock Exchange;*
- *Singapore Exchange Securities Trading Limited;*
- *Stock Exchange of Thailand;*
- *Stockholmsborsen;*
- *SWX Swiss Exchange;*
- *Tokyo Stock Exchange;*
- *Toronto Stock Exchange; and*
- *Wiener Borse AG.*

ANNEX D**TRANSACTIONS LINKED TO LOCATIONS OF CONCERN
(involving financial institutions)**

- *Transactions involving foreign currency exchanges that are followed within a short time by wire transfer of funds to locations of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.);*
- *Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.);*
- *A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern;*
- *The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern;*
- *A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations;*
- *The opening of accounts of financial institutions from locations of specific concern; or*
- *Sending or receiving funds by international transfers from and/or to locations of specific concern.*

ANNEX E

EXAMPLE FOR RATINGS FOR SENSITIVE COUNTRIES

Source	Political & Economic Rating				Money Laundering Rating				Overall Objective Rating	
	Banks own rating	Political Risk	Democracy Ranking	Export risk guarantee (ERG)	TI	Corruption Index	Blocked countries	FATF		FINCEN
Anastasia	4	4	4	4			x			4
Belungia	4	4	3	4						4
Cretonia	3	3	4	3						3
Draconia	1									1
Neverland	4	4	4	4	4		x			4
Fireland	4	4		4						4
Grumpy Islands	3	2	2	3	3					3
Horrorland	4	4	3	4	4					4
Land of Wisdom	2	3	2	2	3					3
Everland	1	1	1	1	1					1
Paradise	1	1	1	1	1					1

Risk Category	low	medium	high
---------------	-----	--------	------

(Source: How to Combat Money Laundering and Terrorist Financing - The Regulator's Guide - Edited by Richard Pratt - Central Banking Publications Ltd.)

ANNEX F

EXAMPLE FOR DUE DILIGENCE PROCESS

	Low Risk	Medium Risk	High Risk
Identification			
Name Check			
Verification			
Client Profile			
Origin of Funds / of Wealth			
Background Search			
Detailed Analysis			

ANNEX G

EXAMPLE FOR APPROVAL PROCESS

Approvals	Low Risk	Medium Risk	High Risk
4 Eyes Approval	CA / Supervisor		
Independent 4 Eye		CA / Super / Compliance	
Senior Man & Independent 4 Eye			CA / Super / Senior Man / Compliance

ANNEX H

EXAMPLE FOR CONTROL PROCESS

Controls	Low Risk	Medium Risk	High Risk
Standard Front	+++	+++	+++
Compliance Control	+	++	+++
Audit	-	+	++
Regulators	-	-	+
	+ Check the Proc	++ Sample Checks	+++ Full Checks

ANNEX I

EXAMPLE FOR CLIENT RISK RATING

RISK FACTOR	DUE DILIGENCE	RISK CATEGORY	
Nationality	Colombian		Risk Category <div style="background-color: #d9ead3; padding: 5px; margin: 5px;">low</div> <div style="background-color: #fff2cc; padding: 5px; margin: 5px;">medium</div> <div style="background-color: #f4cccc; padding: 5px; margin: 5px;">high</div>
Domicile	UK		
Industry	Coffee Table		
Profession	Businessman		
Origin / Souce of Funds	Sale of business		
Complexity	DomCo's/Multiple Relationship		
Asset Volume	80Mo		
Transactions	high/in line with expected		
Overall Rating		medium	

(Source: How to Combat Money Laundering and Terrorist Financing - The Regulator's Guide - Edited by Richard Pratt - Central Banking Publications Ltd.)

ANNEX J

SOURCES OF INFORMATION

Several sources of information exist that may help insurance institutions in determining whether a potentially suspicious or unusual transaction could indicate funds involved in the financing of terrorism and thus be subject to reporting obligations under relevant anti-money laundering or anti-financing of terrorism laws and regulations.

➤ **United Nations lists**

Committee on S/RES/1267(1999) website:

<http://www.un.org/Docs/sc/committees/AfghanTemplate.htm>

➤ **Other lists**

(1) Financial Action Task Force

FATF Identification of Non-Cooperative Countries and Territories

FATF website: http://www.fatf-gafi.org/NCCT_en.htm

(2) United States

Executive Order 13224, 23 September 2001 (with updates)

US Department of the Treasury website :<http://www.ustreas.gov/terrorism.html>

(3) Council of the European Union

Council Regulation (EC) N° 467/2001 of 6 March 2001 [on freezing Taliban funds]

Council Regulation (EC) N° 927/2001 of 27 December 2001 [list of terrorist and terrorist organisations whose assets should be frozen in accordance with Council Regulation (EC) N° 2580/2001]

Council Common Position of 27 December 2001 on application of specific measures to combat terrorism [list of persons, groups and entities involved in terrorist acts]

EUR-lex website:<http://europa.eu.int/eur-lex/en/index.html>

(4) Transparency International

Corruption Perceptions Index

TI website: <http://www.transparency.org> or <http://www.icgg.org>

(5) Swiss Export Risk Insurance

Export Risk Guarantee

SERV website:

<http://www.serv-ch.com/en/deckungspolitik/overall-list-of-countries/index.html>

➤ **Standards**

(1) Financial Action Task Force

FATF Special Recommendations on Terrorist Financing

FATF website: http://www.fatf-gafi.org/TerFinance_en.htm

FATF Forty Recommendations on Money Laundering

FATF website: http://www.fatf-gafi.org/40Recs_en.htm

(2) UN Conventions and Resolutions

International Convention on the Suppression of Terrorist Financing

Website :<http://untreaty.un.org/English/Terrorism.asp>

UN Security Council Resolutions on Terrorism

Website :<http://www.un.org/terrorism/sc.htm>

(3) Council of the European Union

Council Regulation (EC) N° 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism

EUR-lex website:<http://europa.eu.int/eur-lex/en/endex.html>

REPORT FORM TO THE FINANCIAL INTELLIGENCE OFFICE
(Report made under Article 7 of the Administrative Regulation No. 7/2006, of 7 April)

(Main Form)

SUSPICIOUS TRANSACTION REPORT

In accordance with Article 7 of Administrative Regulation No. 7/2006, reporting entity is obliged to report suspicious transaction within 2 working days to Financial Intelligence Office (Portuguese acronym "GIF"), and it is stipulated in Article 9 that non-compliance with the duties established in this administrative regulation constitutes an administrative offence, and is subject to penalty.

Please take note of the followings prior to completing the Suspicious Transaction Report ("STR"):

- **Provide** a clear and concise description to the STR, and **state** all available information.
- **Document** in detail why the transaction is considered extraordinary, irregular or suspicious.
- **Provide** supporting document where is necessary to explain the STR.
- **Indicate** if the potential violation is an initial report or if it relates to a previous transaction or transactions reported.
- **Complete** this STR in Block letters.
- **Take** reference to the explanatory notes below when completing the STR.
- After completion, please **send** this report to the Financial Intelligence Office.

Address: Av. Dr. Mário Soares, nos. 307-323, Edif. "Banco da China", 22 andar "A, B e C"

Contact Telephone Number: 2852 3666

(This box is to be completed by GIF)

Reporting Entity Reference Number: _____

STR Reference Number: _____ / _____

1. Reporting Date and Sequence Number:

/ / N°
 yyyy / mm / dd

2. Type of Transaction Reported: (Please ✓ to select)

- a. Initial Report (Previously reported person/organization? Yes No)
- b. Amendment Report: (1) Partial Amendment
 (2) Replacement
 (3) Cancellation
- c. Supplementary Report

Total Number of document submitted: _____ pages
 (Main Form 4 pages,
 Supplementary Form A _____ pages,
 Supplementary Form B _____ pages,
 Attachment _____ pages,
 Other Document _____ pages)

Previous STR Ref. Number: _____ / _____ Remarks: _____

Section Explanatory Notes

1. **Reporting Date and Sequence Number** is comprised of the date of submitting the STR and the Sequential Number of STR submitted on the same day, eg. 2006/11/01 N° 3 means the 3rd report submitted on 1st November 2006. This reference number is for temporary identification purpose. GIF will assign a unique STR Reference Number for each reported case, and inform reporting entity in writing. Thereafter, the STR Reference Number **must** be quoted when submitting Amendment or Supplementary Report.
- 2a. **Initial Report** refers to first-time reporting of a suspicious transaction/(s), and each report should be made on transaction basis. If this person/organization has been involved in a previously reported case, it should still be reported as an Initial Report, but the earliest STR Number is to be provided in Remarks.
- 2b. **Amendment Report** refers to amendments made to previously submitted STR. Please state the previous STR Reference Number. Type of Amendment includes (1) **Partial Amendment**, (2) **Replacement**, and (3) **Cancellation of STR**. Please fill in the right number in the box of (b). For Partial Amendment, only the amended part is to be completed. Replacement is applicable where the whole set of submitted STR is to be replaced due to significant amendment, but the STR Reference Number remains unchanged. For Cancellation of an STR, a reason must be stated in Remarks.
- 2c. **Supplementary Report** refers to additional information provided to a previously submitted STR, such as recently discovered information or additional person/organization suspected to be involved in the same transaction. For new transaction/(s) related to a previously reported person/organization, it will be filed as an Initial Report (See Note 2a).
6. **Supervisory Authorities** are the competent public departments or professional bodies governing the activities of certain reporting entities. Reporting entities should match themselves with their supervisory authorities.
9. **Person/Organization conducting suspicious transactions** should be classified either as Individual or Corporation/Organization. Corporation is also known as commercial establishment such as proprietorship/partnership/companies whilst Organization is usually set up for specific non-commercial purposes.

NOTE: Please keep a copy of this document, and the following items, for a period of five years:

- All the support documentation, including oral or written reports made by the reporting entities.
- Explanation to this report provided by any other person(s), the identification of such persons(s) and date of the explanation given.

