Guidance Note on Prevention of Money Laundering and Terrorist Financing

October 2010

Office of the Commissioner of Insurance

CONTENTS

PART I OVERVIEW

1. INTRODUCTION

1.1 This Guidance Note aims to prevent criminal use of the insurance industry for the purposes of money laundering and terrorist financing. It presents the background information on money laundering and terrorist financing and summarizes the relevant legislations in Hong Kong. It also sets out the expectation of the Office of the Commissioner of Insurance ("OCI") of the internal policies and procedures of authorized insurers, reinsurers, insurance agents and insurance brokers carrying on or advising on long term business (hereinafter referred to as "insurance institutions") to guard against money laundering and terrorist financing.

1.2 This Guidance Note applies to all insurance institutions which are not financial institutions authorized by the Hong Kong Monetary Authority under the Banking Ordinance (Cap. 155) ("authorized financial institutions"). Insurance institutions that are authorized financial institutions are subject to the Hong Kong Monetary Authority's guidelines on prevention of money laundering ("the HKMA's guidelines"). However, to the extent that there are some insurance specific requirements and examples of suspicious transactions or money laundering cases in this Guidance Note which may not be shown in the HKMA's guidelines, the insurance institutions that are authorized financial institutions are required to have regard to paragraphs 2.2, 5, 6.1-6.3, 6.6.1-6.6.3, 6.7-6.8, 7.2.4 and 8.2.12 as well as Annexes 2, 3, 4 and 5 of this Guidance Note.

1.3 This Guidance Note does not have the force of law and should not be interpreted in any manner which would override the provisions of any applicable law or other regulatory requirements. However, failure to follow the requirements of this Guidance Note by insurance institutions may reflect adversely on the fitness and properness of their directors and controllers. Similarly, failure to follow the requirements of the HKMA's guidelines by the insurance institutions that are authorized financial institutions may reflect adversely on the fitness and properness of their directors and controllers. The OCI may take any appropriate interventionary actions empowered by the Insurance Companies Ordinance (Cap. 41) or other administrative sanctions if an insurance institution is found to be not in compliance with this Guidance Note.

1.4 The scope of this Guidance Note covers the activities of all insurance institutions to the extent that such activities are within the jurisdiction of Hong Kong. Where a Hong Kong incorporated insurance institution has branches or subsidiaries overseas, the requirements also apply to their overseas branches and subsidiaries. Where the local requirements differ

from these requirements, the overseas operations should apply the higher standard to the extent that the local laws permit. Where an overseas branch or subsidiary is unable to observe group standards, the OCI should be informed.

1.5 This Guidance Note will be regularly reviewed and revised in the light of developments in international standards on prevention of money laundering and terrorist financing.

2. BACKGROUND

2.1 What is money laundering and terrorist financing?

2.1.1 Money laundering is the processing of the illicit 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 illegitimate source.

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

2.2 Vulnerabilities in insurance

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

2.2.2 Examples of the type of long term insurance contracts that are vulnerable as a vehicle for laundering money or financing terrorism are products such as:

(a) unit-linked or with profit single premium contracts;

(b) single premium life insurance policies that store cash value;

(c) fixed and variable annuities; and

(d) (second hand) endowment policies.

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

- the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds;

- the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding;

- the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers.

2.2.4 Insurance intermediaries are important for distribution, underwriting and claims settlement. They are often the direct link to the policy holder and therefore, intermediaries should play an important role in anti-money laundering and combating the financing of terrorism. The same principles that apply to insurers should generally apply to insurance intermediaries. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of or does not conform to necessary procedures, or who fails to 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 insurers.

2.3 Stages of money laundering

2.3.1 There are three common stages of money laundering during which numerous transactions may be made by the launderers that could alert an insurance institution to potential criminal activity:

(a) Placement – the physical disposal of cash proceeds derived from illegal activity;

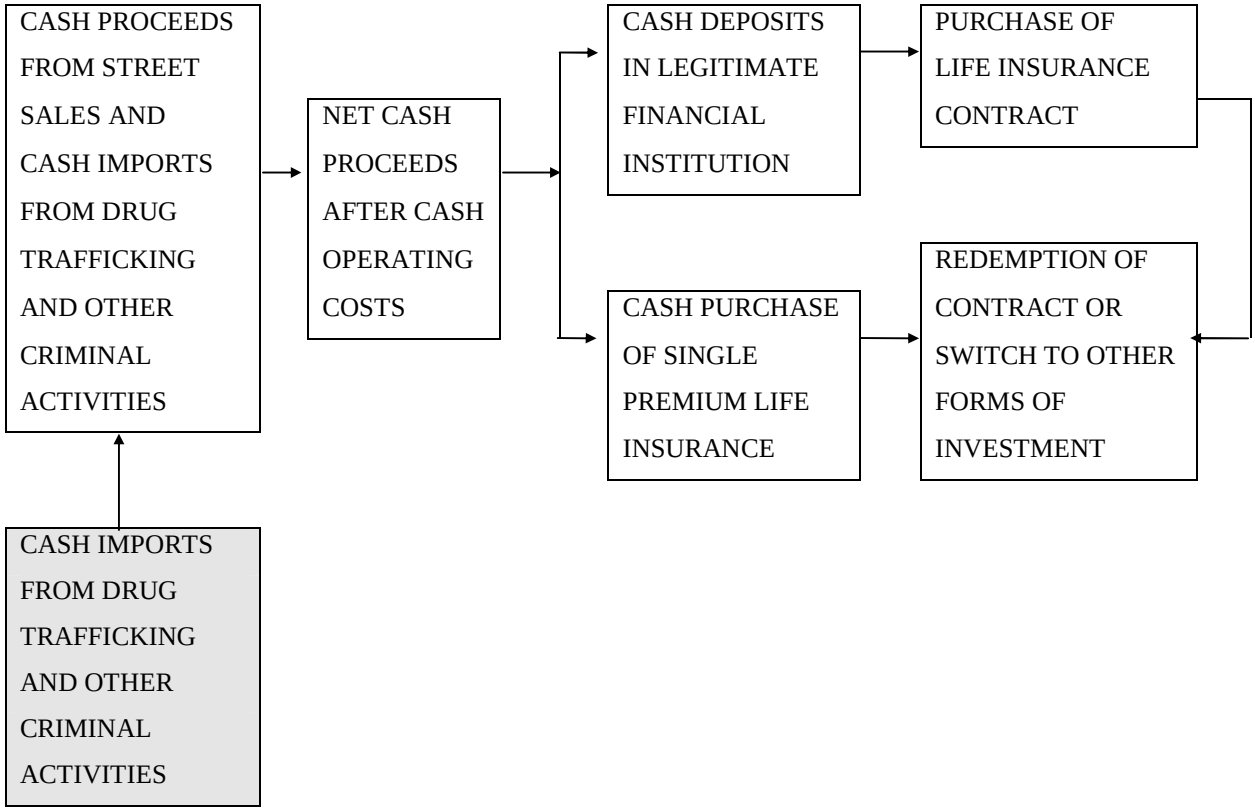
(b) Layering – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity; and

(c) 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.

2.3.2 The following chart illustrates the laundering stages in more detail.

LAUNDERING OF PROCEEDS



Domestic

Foreign

2.4 International initiatives

2.4.1 The Financial Action Task Force ("FATF") was established in 1989 in an effort to thwart attempts by criminals to launder the proceeds of criminal activities through the financial system. In November 1990, Hong Kong was invited to participate as an observer in FATF, and has, since December 1990, attended FATF meetings and played an active role in its deliberations. Hong Kong was admitted as a full member in March 1991.

2.4.2 The FATF has, among other things, put forward 40 Recommendations[1] 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 terrorist financing and promulgated Special Recommendations on Terrorist Financing[2] (further updated in October 2004). These two sets of Recommendations set out the international framework to detect, prevent and suppress money laundering and terrorist financing activities. As a member of the FATF, Hong Kong is obliged to follow the measures in the Recommendations.

2.4.3 To keep in line with the development of prevention of money laundering and terrorist financing standards in the financial sectors, the International Association of Insurance Supervisors ("IAIS") issued a Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism[3] in October 2004 which adapts the standards in the FATF Recommendations to the specific practices and features of the insurance business. The OCI's Guidance Note has taken into account the relevant measures in the FATF Recommendations and the IAIS Guidance Paper.

[1] The 40 Recommendations can be downloaded from FAFT website at ***http://www.fatf-gafi.org***

[2] The Special Recommendations on Terrorist Financing can be downloaded from FAFT website at ***http://www.fatf-gafi.org***

[3] The Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism can be downloaded from IAIS website at ***http://www.iaisweb.org***

3. LEGISLATION

3.1 The legislation concerning money laundering in Hong Kong

3.1.1 Legislation has been enacted in Hong Kong to address problems associated with the laundering of proceeds from drug trafficking and serious crimes. The Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) ("DTROP") provides for the tracing, freezing and confiscation of the proceeds of drug trafficking and creates a criminal offence of money laundering in relation to such proceeds. Under section 4 of DTROP, proceeds are not limited solely to the actual profits of drug sales or distribution, but may constitute any payments or other rewards received by a person at any time in connection with drug trafficking carried on by him or another, and property derived or realized therefrom.

3.1.2 The Organized and Serious Crimes Ordinance (Cap. 455) ("OSCO"), which was modelled on the DTROP, extends the money laundering offence to cover the proceeds of indictable offences in addition to drug trafficking.

3.1.3 The key money laundering provisions in the two Ordinances are summarized below. This does not constitute a legal interpretation of the provisions of the legislation referred to, for which appropriate legal advice should be sought where necessary.

3.1.4 Sections 3 to 5 of the OSCO provide that the Secretary for Justice or an authorized officer, for the purpose of investigating an organized crime, may apply to the Court of First Instance for an order to require a person to provide information or produce material that reasonably appears to be relevant to the investigation. The Court may make an order that the person makes available the material to an authorized officer. An authorized officer may also apply for a search warrant under the OSCO. A person cannot refuse to furnish information or produce material under sections 3 or 4 of the OSCO on the ground of self-incrimination or breach of an obligation to secrecy or other restriction on the disclosure of information imposed by statute or other rules or regulations.

3.1.5 Authorized officer includes any police officer, any member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342); or any officer in the Joint Financial Intelligence Unit ("JFIU") which

was established and is operated jointly by the Police and the Customs and Excise Department.

3.1.6 Section 25(1) of DTROP and OSCO create the offence of dealing with any property, knowing or having reasonable grounds to believe it in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence respectively. The offence carries a maximum sentence of 14 years' imprisonment and a maximum fine of HK$5 million.

3.1.7 It is a defence under section 25(2) of both Ordinances for a person to prove that he intended to disclose as soon as it is reasonable such knowledge, suspicion or matter to an authorized officer or has a reasonable excuse for his failure to make a disclosure in accordance with section 25A(2) of both Ordinances.

3.1.8 Section 25A(1) of both Ordinances impose a statutory duty on a person, who knows or suspects that any property in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence, or was or is intended to be used in that connection, to make a disclosure to an authorized officer as soon as it is reasonable for him to do so. Section 25A(7) of both Ordinances make it an offence for a person failing to make such disclosure. The offence carries a maximum penalty of a fine of HK$50,000 and imprisonment for 3 months.

3.1.9 It should be noted that section 25(4) of OSCO provides that references to an indictable offence in sections 25 and 25A of OSCO include a reference to conduct which would constitute an indictable offence if it had occurred in Hong Kong. That is to say it shall be an offence for a person to deal with the proceeds of crime or fail to make the necessary disclosure under section 25A(1) of OSCO even if the conduct is not committed in Hong Kong, provided that it would constitute an indictable offence if it had occurred in Hong Kong.

3.1.10 Section 25A(2) of both Ordinances provide that if a person who has made the necessary disclosures does any act in contravention of section 25(1) and the disclosure relates to that act, he does not commit an offence if:

(a) the disclosure is made before he does that act and the act is done with the consent of an authorized officer; or

(b) the disclosure is made after the person does the act and the disclosure is made on the person's own initiative and as soon as it is reasonable for him to make it.

3.1.11 Section 25A(3) of both Ordinances provide that disclosure made under section 25A(1) shall not be treated as breach of contract or of any enactment restricting disclosure of information and shall not render the person making the disclosure liable in damages for any loss arising out of disclosure. Therefore, insurance institutions need not fear breaching their duty of confidentiality owed to customers when making a disclosure under the two Ordinances.

3.1.12 Section 25A(4) of both Ordinances provide that a person who is in employment can make disclosure to the appropriate person in accordance with the procedures established by his employer for the making of such disclosure. To the employee, such disclosure has the effect of disclosing the knowledge or suspicion to an authorized officer as required under section 25A(1).

3.1.13 A "tipping-off" offence is created under section 25A(5) of both Ordinances, 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 an investigation into money laundering activities. The "tipping-off" offence carries a maximum penalty of a fine of HK$500,000 and an imprisonment for 3 years.

3.1.14 Insurance institutions may receive restraint orders and charging orders on the property of a defendant of a drug trafficking offence or an offence specified in OSCO. These orders are issued under sections 10 and 11 of the DTROP or sections 15 and 16 of the OSCO. On service of these orders, an authorized officer may require a person to deliver as soon as practicable documents or information, in his possession or control which may assist the authorized officer to determine the value of the property. Failure to provide the documents or information is an offence under DTROP or OSCO. In addition, a person who knowingly deals in any realizable property in contravention of a restraint order or a charging order also commits an offence under DTROP or OSCO.

3.2 The legislation concerning terrorist financing in Hong Kong

3.2.1 The United Nations Security Council ("UNSC") has passed various resolutions to require sanctions against certain designated terrorists and terrorist organizations. In Hong Kong, regulations issued under the United Nations Sanctions Ordinance (Cap. 537) give effect to these UNSC resolutions. In particular, the United Nations Sanctions (Afghanistan) Regulation (Cap. 537K) and the United Nations Sanctions (Afghanistan) (Amendment) Regulation provide, among other things, for a prohibition on making funds available to designated terrorists. The list of designated terrorists is published in the Gazette from time to time.

3.2.2 In addition, the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) ("UNATMO") was enacted in July 2002 and was subsequently amended through the enactment of the United Nations (Anti-Terrorism Measures) (Amendment) Ordinance 2004 in July 2004[4]. The legislation implements the mandatory elements of the UNSC Resolution 1373. The latter aims at combating international terrorism on various fronts, including the introduction of measures against terrorist financing. The UNATMO also implements the most pressing elements of the FATF Special Recommendations.

3.2.3 The key terrorist financing provisions in the amended UNATMO are summarized below. This does not constitute a legal interpretation of the provisions of the legislation referred to, for which appropriate legal advice should be sought when necessary.

3.2.4 Section 7 of the amended UNATMO prohibits the supply or collection of funds to carry out terrorist acts, and section 8 of the amended UNATMO prohibits making funds (or financial) or related services available to terrorists or terrorist associates. Sections 6 and 13 of the amended UNATMO further permit terrorist property to be frozen and subsequently forfeited.

3.2.5 Section 12(1) of the amended UNATMO requires a person to report his knowledge or suspicion of terrorist property to an authorized officer (e.g. the JFIU). Failure to make a disclosure under this section constitutes an offence under section 14(5). The maximum penalty upon conviction of this offence is a fine of HK$50,000 and imprisonment for 3 months.

[4] A substantial part of this Amendment Ordinance has come into operation in January 2005.

3.2.6 The term “funds” includes funds mentioned in Schedule 1 to the amended UNATMO. It covers cash, cheques, claims on money, deposits with financial institutions or other entities, balances on accounts, securities and debt instruments (including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures, debenture stock and derivatives contracts), interest, dividends or other income on or value accruing from or generated by property, letters of credit, documents evidencing an interest in funds or financial resources, etc.

3.2.7 A list of terrorist or terrorist associate names is published in the Gazette from time to time pursuant to section 10 of the United Nations Sanctions (Afghanistan) Regulation and section 4 of the amended UNATMO. The published lists reflect designations made by the United Nations Committee that were established pursuant to UNSC Resolution 1267. The amended UNATMO provides that it shall be presumed, in the absence of evidence to the contrary, that a person specified in such a list is a terrorist or a terrorist associate (as the case may be).

3.2.8 Regarding the obligations under section 12(1) of the amended UNATMO to disclose knowledge or suspicion that property is terrorist property, section 12(2) of the amended UNATMO states that if a person who has made such a disclosure does any act in contravention of section 7 or 8 of the amended UNATMO either before or after such disclosure and the disclosure relates to that act, the person does not commit an offence if:

(a) the disclosure is made before he does that act and he does that act with the consent of the authorized officer; or

(b) the disclosure is made after he does that act, is made on his own initiative and is made as soon as it is practicable for him to make it.

3.2.9 Section 12(3) provides that a disclosure made under the amended UNATMO shall not be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, rule of conduct or other provision. The person making the disclosure shall not be liable in damages for any loss arising out of the disclosure or any act done or omitted to be done in relation to the property concerned in consequence of the disclosure.

3.2.10 Section 12(4) of the amended UNATMO provides that a person who is in employment can make disclosure to the appropriate person in accordance with the procedures established by his employer for the making of such disclosure. To the employee, such disclosure has the effect of disclosing the knowledge or suspicion to an authorized officer as required under section 12(1).

3.2.11 Sections 12A, 12B and 12C of the amended UNATMO provide that the Secretary for Justice or an authorized officer, for the purpose of investigating an offence under the Ordinance, may apply to the Court of First Instance for an order to require a person to provide information or produce material that reasonably appears to be relevant to the investigation. The Court may make an order that the person makes available the material to an authorized officer. An authorized officer may also apply for a search warrant under the amended UNATMO. A person cannot refuse to furnish information or produce material under section 12A or 12B of the amended UNATMO on the ground of breaching an obligation to secrecy or other restriction on the disclosure of information imposed by statute or other rules or regulations.

4. POLICIES AND PROCEDURES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

4.1 The senior management of an insurance institution should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness. The OCI expects that insurance institutions should have in place the following policies, procedures and controls:

(a) Insurance institutions should issue a clear statement of group policies in relation to money laundering and terrorist financing and communicate the group 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
- Staff screening and training

based on the guidance in Part II of this Guidance Note.

(c) Insurance institutions should comply with relevant legislations and seek actively to promote close co-operation with law enforcement authorities.

(d) 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 terrorist financing activities.

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

(f) 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 terrorist financing and, where appropriate, have been instructed to report to the local reporting point for their suspicions.

PART II DETAILED GUIDELINES

5. CUSTOMER ACCEPTANCE

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

5.2 Insurance institutions should develop customer acceptance policies and procedures that aim to identify the types of customers[5] and/or beneficial owners[6] that are likely to pose a higher than average risk of money laundering and terrorist financing. 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.

5.3 In assessing the risk profile of a customer relationship, an insurance institution should consider the following factors[7]:

(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) the customer's and/or beneficial owner's nationality, citizenship and resident status (in the case of a corporate customer, the customer's place of incorporation), the place where the customer's and/or beneficial owner's business is established, the location of the counterparties with whom the customer and/or beneficial owner conducts business, and whether the customer and/or beneficial owner is otherwise connected with higher risk jurisdictions or jurisdictions which do not or insufficiently apply the FATF Recommendations (paragraph 6.6.6), or which are known to the insurance institution to be lack of proper standards in the prevention of money laundering

[5] For the purpose of this Guidance Note, the term "customer" refers to policy holder.

[6] For the purpose of this Guidance Note, the term "beneficial owner" refers to the owner/controller of the policy holder, i.e. the natural person(s) who ultimately owns or controls a policy holder/potential policy holder or the person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

[7] 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 this Guidance Note).

or customer due diligence process;

(d) background or profile of the customer and/or beneficial owner, such as being, or linked to, a politically exposed person (paragraph 6.6.5);

(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) for a corporate customer and/or beneficial owner, unduly complex structure of ownership for no good reason;

(g) 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);

(h) the source of funds/wealth;

(i) the delivery mechanism, or distribution channel, used to sell the product (e.g. non face-to-face transactions (paragraph 6.6.4), business sold through insurance intermediaries (paragraph 6.8)); 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 another financial institution).

5.4 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.

6. CUSTOMER DUE DILIGENCE

6.1 General principle

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

(a) identify the customer and/or beneficiary and verify the customer's and/or beneficiary's identity using reliable, independent source documents, data or information;

(b) ask and determine whether the customer is acting on behalf of another person for the purpose of identifying the insured and/or beneficial owner, and then take reasonable steps to obtain sufficient identification data to verify the identity of that other person, if applicable;

(c) identify the beneficial owner and take reasonable measures to 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 take reasonable measures to understand the ownership and control structure of the customer;

(d) obtain information on the purpose and intended nature of the business relationship between the customer and the insurance institution; and

(e) 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.

6.1.2 Unwillingness of the customer, for no good reason, to provide the information requested and to cooperate with the insurance institution's customer due diligence process may itself be a factor that should trigger suspicion.

6.1.3 The general rule is that customers and/or beneficial owners and/or beneficiaries 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 and/or beneficiary, business relationship or transaction (factors for deciding the risk profile are set out in paragraph 5.3). Enhanced due diligence is called for with respect to higher risk categories. Conversely, it is acceptable for insurance institutions to apply simplified due diligence for lower risk categories as outlined in paragraphs 6.1.4, 6.3.2 and 6.3.4. Specific customer due diligence requirements applicable to different types of customers are outlined in paragraphs 6.2 to 6.7.

6.1.4 In general, insurance institutions may apply simplified due diligence in respect of a corporate customer where there is no suspicion of money laundering and terrorist financing, and:

- the risk of money laundering and terrorist financing is assessed to be low; or
- there is adequate public disclosure in relation to the customers; or
- there are adequate checks and controls exist elsewhere in national systems.

6.1.5 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 and/or beneficiaries. 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 OCI or any other relevant authority. Among other things, this would require the insurance institution to document its assessment and the reasons for it.

6.1.6 If claims, commissions, and other monies are to be paid to persons or companies other than the customers or beneficiaries, then the proposed recipients of these monies should also be the subjects of identification and verification.

6.1.7 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, the findings established in writing, and be available to help competent authorities. 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.

6.1.8 As to reinsurance, due to the nature of the business and the lack of a contractual relationship between the policy holder and the reinsurer, it is often impractical for the reinsurer to carry out verification of the policy holder and/or the beneficial owner and/or the beneficiary. Therefore, for reinsurance business, reinsurers should only have business with ceding insurers that are authorized and supervised by the OCI or an equivalent authority in a jurisdiction that is a FATF member or that applies standards of prevention of money laundering and terrorist financing equivalent to those of the FATF.

6.1.9 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.

6.1.10 Insurance institutions may permit the identification of beneficiary to take place after having established the business relationship, provided that the money laundering risks and financing of terrorism risks are effectively managed. Notwithstanding the above, the verification of the beneficiary should occur at the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

6.1.11 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.

6.1.12 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.

6.1.13 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. The return of premiums should be subject to any request from the JFIU to freeze the relevant premiums.

6.2 Individuals

6.2.1 Insurance institutions should institute effective procedures for obtaining satisfactory evidence of the identity of individual customers and/or beneficial owners and/or beneficiaries including obtaining information about:

(a) true name and/or name(s) used;
(b) identity card/passport number;
(c) current permanent address;
(d) date of birth;
(e) nationality[8]; and
(f) occupation/business[9].

6.2.2 Identification documents such as current valid passports or identity cards should be produced as identity proof. For Hong Kong residents, the prime source of identification will be the identity cards. File copies of identification documents should be retained.

6.2.3 In principle, copies of the identification documents of individual customers should be collected before, or at the moment when, the insurance contract is concluded. However, as far as an individual beneficiary is concerned, copy of his/her identification document should only be collected at the time of payout or the time when he/she intends to exercise vested rights under the policy.

6.2.4 Having considered the difficulty for insurance institutions to obtain copies of the identification documents of individual customers when the sales process occurs outside the office, insurance institutions may obtain and keep copies of the identification documents after having established the business

[8] For an individual who is a holder of Hong Kong Permanent Identity Card, the verification of nationality is not mandatory.

[9] Information about occupation/business is a relevant piece of information about a customer and/or beneficial owner and/or beneficiary but does not form part of the identification information requiring verification.

relationship provided that the money laundering risks and financing of terrorism risks are effectively managed. In all such circumstances, copies of identification documents of individual customers 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 6.1.11 provides guidance for adopting the risk management procedures.

6.2.5 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 the Immigration Department or the relevant consulates in Hong Kong to ascertain whether the details on the document are correct.

6.2.6 Insurance institutions should check the address [10] of the applicant by appropriate means, e.g. by requesting sight of a recent utility or rates bill or a recent bank statement.

6.2.7 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 5.3.

6.3 Corporations

6.3.1 The following documents or information should be obtained in respect of corporate customers and/or beneficial owners and/or beneficiaries which are registered in Hong Kong, not being financial institutions as mentioned in paragraph 6.3.4 (comparable documents, 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 and/or beneficiaries which are not registered in Hong Kong, not being financial institutions as mentioned in paragraph 6.3.4):

(a) copies of certificate of incorporation and business registration certificate;

[10] Insurance institutions should, however, use a common sense approach to handle cases where the customers and/or beneficial owners (e.g. students and housewives) are unable to provide address proof. Apart from the method suggested in paragraph 6.2.5, insurance institutions may use other appropriate means, such as home visits, to verify the residential address of a customer and/or beneficial owner.

(b) copies of memorandum and articles of association (if insurance institution considers necessary having regard to the risk of the particular transaction);

(c) copy of 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;

(d) a search of the file at Companies Registry, if there is a suspicion about the legitimacy of the legal entity.

6.3.2 It will generally be sufficient for an insurance institution to adopt simplified due diligence in respect of a corporate customer and/or beneficial owner and/or beneficiary by obtaining the documents specified in paragraph 6.3.1 if the risk of money laundering and terrorist financing is assessed to be low. Some examples of lower risk corporate customers and/or beneficial owners and/or beneficiaries are:

(a) the company is listed in Hong Kong or on a recognized stock exchange (Annex 1) (or is a subsidiary of such listed company);

(b) the company is a state-owned enterprise in a jurisdiction where the risk of money laundering is assessed to be low and where the insurance institution has no doubt as regards the ownership of the enterprise;

(c) the company acquires an insurance policy for pension schemes which does not have surrender clause and the policy cannot be used as collateral; or

(d) 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.

6.3.3 Where a listed company 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).

6.3.4 Where a corporate customer and/or beneficial owner and/or beneficiary is a financial institution which is authorized and supervised by the OCI, HKMA, the Securities and Futures

Commission of Hong Kong or an equivalent authority in a jurisdiction that is a FATF member or that applies standards of prevention of money laundering and terrorist financing 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.

6.3.5 In relation to a corporate customer and/or beneficial owner and/or beneficiary which does not fall into the descriptions of paragraphs 6.3.2 and 6.3.4, 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 6.3.1, 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 rights of a company), at least two directors[11] (including the managing director) of the company and all authorized signatories designated to sign insurance contracts. The insurance institution should also identify the source of funds. Besides, a search of the file at Companies Registry should be performed.

6.3.6 Where a corporate customer which does not fall into the descriptions of paragraphs 6.3.2 and 6.3.4; 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.

6.3.7 An insurance institution should understand the ownership structure of non-listed corporate customers and determine the source of funds. An unduly complex ownership structure for no good reason is a risk factor to be taken into account (paragraph 5.3 (f)).

6.3.8 An insurance institution should exercise special care in initiating business transactions with companies that have

[11] In case of one-director companies, insurance institutions are only required to verify the identity of that director.

nominee shareholders. Satisfactory evidence of the identity of beneficial owners of such companies should be obtained.

6.3.9 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.

6.3.10 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.

6.4 Unincorporated businesses

6.4.1 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 paragraph 6.2. 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.

6.5 Trust accounts

6.5.1 Where trusts or similar arrangements are used, particular care should be taken in understanding the substance and form of the entity. Accordingly, insurance institutions should always establish, by confirmation from an applicant for insurance policy, whether the applicant is acting on behalf of another person as trustee, nominee or agent. 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 settlors[12] and the beneficiaries[13]. Should it

[12] When the verification of the identity of the settlor is not possible, insurance institutions may accept a declaration from the trustee or other contractual party to confirm the link or relationship with the settlor.

[13] 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 undertake

not be possible to verify the identity of the beneficiaries when the policy is taken out, verification of the beneficiaries should be carried out prior to any payments being made to them.

6.5.2 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.

6.6 Higher risk customers

6.6.1 Insurance institutions should apply an enhanced due diligence in respect of higher risk customers and/or beneficial owners and/or beneficiaries. Some examples of higher risk customers and/or beneficial owners and/or beneficiaries are:

- customers and/or beneficial owners are assessed to be of higher risk based on the factors set out in paragraph 5.3;
- customers of non-face-to-face transactions;
- politically exposed persons as well as persons or companies clearly related to them; or
- customers and/or beneficial owners and/or beneficiaries in connection with jurisdictions which do not or insufficiently apply the FATF Recommendations.

6.6.2 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 on-

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 terrorist financing. A decision not to undertake verification should be approved by senior management.

going 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.

6.6.3 Apart from the above general additional measures, specific additional measures are also applicable to the customers of non-face-to-face transactions (paragraph 6.6.4); customers who are classified as politically exposed persons (paragraph 6.6.5); and customers in connection with jurisdictions which do not or insufficiently apply the FATF Recommendations (paragraph 6.6.6).

6.6.4 New or developing technologies: Customers of non-face-to-face transactions

6.6.4.1 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 (paragraph 6.8).

6.6.4.2 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.

6.6.4.3 New or developing technologies that might favour anonymity can be used to market insurance products. E-commerce or sales through internet is an example. Where face-to-face interview is not conducted, for example where the account is opened via the internet, an insurance institution should apply equally effective customer identification procedures and on-going monitoring standards as for face-to-face customers.

6.6.4.4 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 satisfies the criteria in paragraph 6.8;

(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.

6.6.5 Politically exposed persons ("PEPs")

6.6.5.1 PEPs are defined as individuals who are or have been entrusted with prominent public functions outside Hong Kong, such as 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. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. 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.

6.6.5.2 Business relationships with PEPs as well as persons or companies clearly related to them (i.e. 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 and people and companies that are clearly related to them. The following CDD measures applicable to PEPs also apply to persons or companies that are clearly related to them.

6.6.5.3 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.

6.6.5.4 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. Where a customer has been accepted and the customer and/or beneficial owner and/or beneficiary is subsequently found to be or become a PEP, an insurance institution should obtain senior management approval to continue the business relationship.

6.6.5.5 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 holds his public office or has been entrusted with his public functions, taking into account his position;

(b) any unexplained sources of wealth or income (i.e. 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.

6.6.5.6 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).

6.6.5.7 While paragraph 6.6.5.1 defines PEPs as individuals who hold prominent public functions outside Hong Kong, insurance institutions are encouraged to extend the relevant requirements on PEPs to individuals who hold prominent public functions in Hong Kong.

6.6.6 Jurisdictions which do not or insufficiently apply the FATF Recommendations

6.6.6.1 An insurance institution should apply Recommendation 21 of the FATF's revised Forty Recommendations to jurisdictions which do not or insufficiently apply the FATF Recommendations. 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."

6.6.6.2 Extra care should therefore be exercised by an insurance institution in respect of customers and/or beneficial owners and/or beneficiaries connected with jurisdictions which do not or insufficiently apply the FATF Recommendations or otherwise pose a higher risk to an insurance institution. In addition to ascertaining and documenting the business rationale for applying for insurance services as required under paragraph 6.1.1 (d)

above, an insurance institution should be fully satisfied with the legitimacy of the source of funds of such customers.

6.6.6.3 Factors that should be taken into account in determining whether jurisdictions do not or insufficiently apply the FATF Recommendations or otherwise pose a higher risk to an insurance institution include:

(a) whether the jurisdiction is, or a significant number of persons or entities in that jurisdiction are, subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances, a jurisdiction subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, may be given credence by an insurance institution because of the standing of the issuer and the nature of the measures;

(b) whether the jurisdiction is identified by credible sources as lacking appropriate anti-money laundering and counter-terrorist financing laws, regulations and other measures;

(c) whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organizations operating within it; and

(d) whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.

"Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supranational or international bodies such as the International Monetary Fund ("IMF"), and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organizations. The information provided by these credible sources does not have the effect of law or regulation and should

not be viewed as an automatic determination that something is of higher risk.

6.6.6.4 In assessing whether or not a jurisdiction (other than FATF members as shown in Annex 1) sufficiently applies FATF standards in combating money laundering and terrorist financing and meets the criteria for an equivalent jurisdiction, insurance institutions should:

(a) carry out their own jurisdiction assessment of the standards of prevention of money laundering and terrorist financing. This could be based on the insurance institutions' knowledge and experience of the jurisdiction concerned or from market intelligence. The higher the risk, the more stringent the due diligence measures that should be applied when undertaking business with a customer from the jurisdiction concerned; and

(b) pay particular attention to assessments that have been undertaken by standard setting bodies such as the FATF and by international financial institutions such as the IMF. In addition to the mutual evaluations carried out by the FATF and FATF-style regional bodies, as part of their financial stability assessments of countries and territories, the IMF and the World Bank have carried out country assessments in relation to compliance with prevention of money laundering and terrorist financing standards based on the FATF Recommendations.

(c) maintain an appropriate degree of on-going vigilance concerning money laundering risks and to take into account information that is reasonably available to them about the standards of anti-money laundering systems and controls that operate in the country with which any of their customers are associated.

6.6.6.5 For jurisdictions with serious deficiencies in applying the FATF Recommendations and where inadequate progress has been made to improve their position, the FATF may recommend the application of further counter-measures. The specific counter-measures, to be determined by the OCI in each case, would be gradual and proportionate to the specific problem of the

jurisdiction concerned. The measures will generally focus on more stringent customer due diligence and enhanced surveillance/reporting of transactions. An insurance institution should apply the counter-measures determined by the OCI from time to time.

6.6.6.6 An insurance institution should be aware of the potential reputation risk of conducting business in jurisdictions which do not or insufficiently apply the FATF Recommendations or other jurisdictions known to apply inferior standards for the prevention of money laundering and terrorist financing.

6.6.6.7 If an insurance institution incorporated in Hong Kong has operating units in such jurisdictions, care and on-going vigilance should be taken to ensure that effective controls on prevention of money laundering and terrorist financing are implemented in these units. In particular, the insurance institution should ensure that the policies and procedures adopted in such overseas units are equivalent to those adopted in Hong Kong. There should also be compliance and internal audit checks by staff from the head office in Hong Kong. In extreme cases the insurance institution should consider withdrawing from such jurisdictions.

6.7 On-going due diligence on existing customers and/or beneficial owners

6.7.1 Insurance institutions should take reasonable steps to ensure that the records of existing customers remain up-to-date and relevant. To achieve this, insurance institutions should perform on-going due diligence on the existing business relationship to consider re-classifying a customer as high or low risk. 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 programme should be established in such a way that insurance institutions are able to adequately gather and analyze information.

6.7.2 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 policy holder;

(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 policy holder 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 a suspicion of money laundering and terrorist financing.

6.7.3 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.

6.7.4 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 5.3.

6.8 Reliance on insurance intermediaries[14] for customer due diligence

6.8.1 Insurers, appointed insurance agents and authorized insurance brokers all have the responsibility to comply with the requirements relating to customer due diligence and record keeping as specified in paragraphs 6 and 7 of this Guidance Note. However, insurance intermediaries, that is agents and brokers, are usually the first line of contacts with the customer, before the customer is known, introduced or referred to an insurer. These insurance intermediaries may actually obtain the appropriate verification evidence in respect of the customer. To avoid duplication of efforts and unnecessary inconvenience to the customer, the insurer may rely on these insurance intermediaries to carry out part or all of the customer due diligence requirements.

6.8.2 For insurers which rely on insurance intermediaries to carry out part or all of the customer due diligence requirements, they must understand their related AML/CFT obligations in respect to these requirements. The ultimate responsibility for customer

[14] Insurance intermediaries refer to appointed insurance agents or authorized insurance brokers carrying on or advising on long term insurance business in Hong Kong.

identification and verification remains with the insurer relying on insurance intermediaries. The insurer concerned should therefore determine whether the intermediary in question possesses an acceptable level of reliability. In this regard, the following criteria should be used:

(a) the customer due diligence procedures of the insurance intermediary should be as rigorous as those which the insurer would have conducted itself for the customer and/or beneficial owner and/or beneficiary in accordance with paragraph 6 of this Guidance Note; and

(b) the insurer must satisfy itself as to the reliability of the systems put in place by the insurance intermediary to verify the identities of the customer and/or beneficial owner and/or beneficiary.

6.8.3 The insurer is expected to conduct periodic reviews to ensure that an insurance agent upon which it relies continues to conform to the criteria set out above. This may involve review of the relevant policies and procedures of the insurance agent and sample checks of the due diligence conducted.

6.8.4 Where reliance on insurance intermediaries for customer due diligence is permitted, the insurer should immediately obtain the necessary information concerning the relevant identification data and other documentation pertaining to the identity of the customer and/or beneficial owner and/or beneficiary from the insurance intermediary. The insurance intermediary should submit such information to the insurer upon request without delay.

6.8.5 The purpose of obtaining the underlying documentation is to ensure that it is immediately available on file for reference purposes by the insurer or relevant authorities such as the OCI and the JFIU, and for on-going monitoring of the customer and/or beneficial owner. It will also enable the insurer to verify that the insurance intermediary is doing its job properly. It is not the intention that the insurer should use the documentation, as a matter of course, to repeat the due diligence conducted by the insurance intermediary.

6.8.6 The insurer should undertake and complete its own verification of the customer and/or beneficial owner and/or beneficiary if it has any doubts about the ability of the insurance intermediary to undertake appropriate due diligence.

7. RECORD KEEPING

7.1 Requirements of the investigating authorities

7.1.1 The DTROP and the OSCO entitle the Court to examine all relevant past transactions to assess whether the defendant has benefited from drug trafficking or other indictable offences.

7.1.2 The investigating authorities need to ensure a satisfactory audit trail for suspected drug related or other laundered money and to be able to establish a financial profile of the suspected account.

7.1.3 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.

7.2 Retention of records

7.2.1 Insurance institutions should keep records on the risk profile of each customer and/or beneficial owner and/or beneficiary and the data obtained through the customer due diligence 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 six years after the end of the business relationship.

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

7.2.3 Insurance institutions should ensure that documents, data or information collected under the customer due diligence process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

7.2.4 Insurance institutions should ensure that they have in place adequate procedures:

(a) to provide initial proposal documentation including, where applicable, the customer financial assessment, analysis of needs, details of the payment method, illustration of benefits, and copy of documentation in support of verification by the insurance institutions;

(b) to retain all records associated with the maintenance of the contract post sale, up to and including maturity of the contract; and

(c) to provide details of the maturity processing and/or claim settlement which will include completed "discharge documentation".

7.2.5 Retention may be by way of original documents, stored on microfiche, or in computerized form provided that such forms are accepted as evidence under sections 20 to 22 of the Evidence Ordinance (Cap. 8). In situation where the records relate to on-going 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.

8. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

8.1 Recognition of suspicious transactions

8.1.1 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. In this regard, insurance institutions are encouraged to adopt the "SAFE" approach as recommended by the JFIU. Details of the "SAFE" approach are set out in Annex 2.

8.1.2 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.

8.1.3 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.

8.1.4 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.

8.1.5 To facilitate the identification of suspicious transactions, indicators of suspicious transactions are given in Annex 3 and examples of money laundering schemes involving life insurance industry are given in Annex 4. The indicators are not intended to be exhaustive and are for reference only. Identification of any of the types of transactions listed in Annex 3 should prompt further investigation and be a catalyst towards making at least initial enquiries about the source of funds.

8.1.6 In relation to terrorist financing, the FATF issued in April 2002 a Guidance for Financial Institutions in Detecting

Terrorist Financing[15]. The document describes the general characteristics of terrorist financing with case studies illustrating the manner in which law enforcement agencies were able to establish a terrorist financing link based on information reported by financial institutions. Annex 3 of the document contains a series of characteristics of financial transactions that have been linked to terrorist activity in the past. An insurance institution should acquaint itself with the FATF paper.

8.1.7 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.

8.1.8 Such database should, in particular, include the lists published in the Gazette[16] under the relevant legislation and those designated under the US President's Executive Order 13224[17]. 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.

8.1.9 An insurance institution should check the names of existing customers and/or beneficial owners and/or beneficiaries 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 terrorist financing. Enhanced checks should be conducted before processing a transaction, where possible, if there are circumstances giving rise to suspicion.

8.2 Reporting of suspicious transactions

8.2.1 The reception point for disclosures under the DTROP, the OSCO and the UNATMO is the JFIU, which is operated jointly by the Police and the Customs and Excise Department.

8.2.2 In addition to acting as the point for receipt of disclosures made by any organization or individual, the JFIU also acts as

[15] The Guidance for Financial Institutions in Detecting Terrorist Financing can be downloaded from FATF website at ***http://www.fatf-gafi.org/dataoecd/39/21/34033955.pdf***

[16] The Gazette can be downloaded from the website of the Government Logistics Department at ***http://www.gld.gov.hk/cgi-bin/gld/egazette/index.cgi?lang=e&agree=0***

[17] Lists designated under the US President's Executive Order 13224 can be downloaded from the United States Department of the Treasury website at ***http://www.ustreas.gov/offices/enforcement/ofac/programs/terror/terror.pdf***

domestic and international advisors on money laundering and terrorist financing generally and offers practical guidance and assistance to the financial sector on the subject of money laundering and terrorist financing.

8.2.3 The obligation to report is on the individual who becomes suspicious of a money laundering or a terrorist financing transaction. Each insurance institution should appoint a designated officer ("compliance officer") at the management level who should be responsible for reporting to the JFIU where necessary in accordance with the relevant legislation and to whom all internal reports should be made.

8.2.4 The role 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. 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.

8.2.5 Where an employee of an insurance institution becomes suspicious of a customer and/or beneficial owner and/or beneficiary, transaction or property, he must promptly report to the compliance officer.

8.2.6 The compliance officer should form a considered view on whether unusual or suspicious transactions should be promptly reported to the JFIU. In reporting to the JFIU, the compliance officer should ensure that all relevant details are provided in the report and cooperate fully with the JFIU for the purpose of investigation. If a decision is made not to report an apparently suspicious transaction to the JFIU, the reasons for this should be fully documented by the compliance officer. The fact that a report may already have been filed with the JFIU in relation to previous transactions of the customer and/or beneficial owner and/or beneficiary in question should not necessarily preclude the making of a fresh report if new suspicions are aroused.

8.2.7 The compliance officer should keep a register of all reports made to the JFIU and all reports made to him by employees. The compliance officer should provide employees with a written acknowledgement of reports made to him, which will

form part of the evidence that these reports were made in compliance with the internal procedures.

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

8.2.9 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.

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

8.2.11 Internal audit also has an important role to play in independently evaluating on a periodic basis an insurance institution's policies and procedures in combating money laundering and terrorist financing. This should include checking the effectiveness of the compliance officer 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 to the prevention of money laundering and terrorist financing 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.

8.2.12 The use of a standard format for reporting (or adaptation of the format) is encouraged (Annex 5). In the event that urgent disclosure is required, an initial notification should be made by telephone. The contact details of the JFIU are at Annex 6.

8.2.13 The JFIU will acknowledge receipt of any disclosure made. If there is no imminent need for action e.g. the issue of a restraint order on an account, consent will usually be given for the institution to operate the account under the provisions of section 25A(2) of both the DTROP and the OSCO, or section 12(2) of

the UNATMO. An example of such a letter is shown at Annex 7 to this Guidance Note.

8.2.14 Insurance institutions should refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have informed the JFIU which consents to the institutions carrying out the transactions. Where it is impossible to refrain or if this is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, institutions may carry out the transactions and notify the JFIU on their own initiative and as soon as it is reasonable for them to do so.

8.2.15 Access to the disclosed information is restricted to financial investigating officers within the Police and the Customs and Excise Department. In the event of a prosecution, production orders will be obtained to produce the material for the Court. Section 26 of the DTROP and the OSCO place strict restrictions on revealing the identity of the person making disclosure under section 25A.

8.2.16 Whilst there are no statutory requirements to provide feedback arising from investigations, the Police and the Customs and Excise Department recognize the importance of having effective feedback procedures in place. The JFIU may, on request, provide to a disclosing institution a status report on the disclosure.

8.2.17 Enhancing and maintaining the integrity of the relationship which has been established between law enforcement agencies and insurance institutions is considered to be of paramount importance.

9. STAFF SCREENING AND TRAINING

9.1 Screening

9.1.1 Insurance institutions should identify the key positions within their organizations with respect to anti-money laundering and combat of terrorist financing 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; and

(b) verification as to whether the information and references provided by the employee are correct and complete.

9.1.2 Insurance institutions should keep records on the identification data obtained from their employees mentioned in paragraph 9.1.1. The records should demonstrate the due diligence performed in relation to the fit and proper requirements.

9.2 Training

9.2.1 Staff must be aware of their own personal obligations under the DTROP, the OSCO and the UNATMO and that they can be personally liable for failing to report information to the authorities. They are advised to read the relevant sections of the DTROP, the OSCO and the UNATMO. They must be encouraged to co-operate fully with the law enforcement agencies and to provide prompt notice of suspicious transactions. They should be advised to report suspicious transactions to their institution's compliance officer if they do not know precisely what the underlying criminal activity is or whether illegal activities have occurred.

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

9.2.3 Timing and content of training packages for various sectors of staff will need to be adapted by individual insurance institutions for their own needs. However, it is recommended that the following might be appropriate:

(a) New employees

A general appreciation of the background to money laundering and terrorist financing, 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 suspicions 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 brokers) are the first point of contact with those who may commit money laundering or terrorist financing offence and the efforts of such staff are therefore vital to the strategy in the fight against money laundering and terrorist financing. 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 suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. It is vital that "front-line" staff are made aware of the insurance institution's policy for dealing with non-regular customers 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 proposer 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) Management

A higher level of instruction covering all aspects of policies and procedures on prevention of money laundering and terrorist financing should be provided to those with the responsibility for supervising or managing staff and for auditing the system. The training will include their responsibility regarding the relevant policies and procedures, the offences and penalties arising from the DTROP, the OSCO and the UNATMO, internal reporting procedures and the requirements for verification and record keeping.

(e) Compliance officers

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

(f) On-going 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 recognizing and reporting suspected money laundering or terrorist financing transactions.

RECOGNIZED STOCK EXCHANGE

Stock exchange of a country which is a member of FATF or a specified stock exchange as defined under the Securities and Futures Ordinance (Cap. 571) (but excluding exchanges in jurisdictions which do not or insufficiently apply the FATF Recommendations)

FATF members

Argentina
Australia
Austria
Belgium
Brazil
Canada
China
Denmark
Finland
France
Germany
Greece
Hong Kong, China
Iceland
India
Ireland
Italy
Japan
Luxembourg
Mexico
Kingdom of the Netherlands
New Zealand
Norway
Portugal
Republic of Korea
Russian Federation
Singapore
South Africa
Spain
Sweden
Switzerland
Turkey
United Kingdom
United States

Specified stock exchanges in non-FATF countries

Kuala Lumpur Stock Exchange
Stock Exchange of Thailand
Philippine Stock Exchange, Inc.

"SAFE" APPROACH RECOMMENDED BY THE JOINT FINANCIAL INTELLIGENCE UNIT

The "SAFE" Approach is an effective systemic approach to identify suspicious financial activity which involves the following four steps:

(a) Step one: **S**creen the account for suspicious indicators: Recognition of a suspicious activity indicator or indicators
(b) Step two: **A**sk the customer appropriate questions
(c) Step three: **F**ind out the customer's records: Review of information already known when deciding if the apparently suspicious activity is to be expected
(d) Step four: **E**valuate all the above information: Is the transaction suspicious?

Examination of the Suspicious Transactions Reporting ("STR") received by the JFIU reveals that many reporting institutions do not use the system outlined above. Commonly, institutions make a STR merely because a suspicious activity indicator has been recognized, i.e. only step one of the systemic approach is followed, steps two, three and four are not followed. This failure to use the systemic approach leads to a lower quality of STRs.

Each of the four steps of the systemic approach to suspicious activity identification is discussed in more detail in the following paragraphs. Insurance institutions should consider carefully the specific nature of their business, organizational structure, type of customer and transaction, etc. when designing their own systems for implementing the respective steps.

Step one: **S**creen the account for suspicious indicators: Recognition of a suspicious activity indicator or indicators

The recognition of an indicator, or better still indicators, of suspicious financial activity is the first step in the suspicious activity identification system. A list of suspicious activity indicators commonly seen within the insurance sector is shown at Annex 3.

Insurance institutions can use different methods in the recognition of suspicious activity indicators. The measures summarized below are recognized as contributing towards an effective overall approach to suspicious activity identification.

(a) Train and maintain awareness levels of all staff in suspicious activity identification.

This approach is most effective in situations in which staff have face-to-face contact with a customer who carries out a particular transaction which displays suspicious activity indicators. However,

this approach is much less effective in situations in which either, there is no face-to-face contact between customer and staff, or the customer deals with different staff to carry out a series of transactions which are not suspicious if considered individually.

(b) Identification of areas in which staff/customer face-to-face contact is lacking (e.g. sales through internet) and use of additional methods for suspicious activity identification in these areas.

(c) Use of a computer programme to identify accounts showing activity which fulfils predetermined criteria based on commonly seen money laundering methods.

(d) Insurance institutions' internal inspection system to include inspection of STR.

(e) Identification of "High Risk" customers, i.e. customers of the type which are commonly high risk in nature, e.g. PEP. Greater attention is paid to monitoring of the activity of these customers for suspicious transactions.

(f) Flagging of customers of special interest on the computer. Staff carrying out future transactions will notice the "flag" on their computer screens and pay extra attention to the transactions conducted by the customer. Customers to be flagged are those in respect of which a suspicious transaction report has been made and/or customers of high risk nature.

A problem with flagging is that staff who come across a large transaction involving a flagged customer may tend to make a report to the compliance officer whether or not the transaction is suspicious. This has the effect of overburdening compliance officers with low quality reports. Flagging may also lead to staff believing that if a customer is not flagged it is not suspicious. Staff must be educated on the proper usage of flagging if it is to work properly.

(g) Adopt more stringent policies in respect of customers who are expected to pay in large amount of cash or to purchase single premium policies, e.g. request customers for the expected nature of transactions and source of funds when establishing business relationship.

Step two: **A**sk the customer appropriate questions

If staff carry out a transaction or transactions for a customer bearing one or more suspicious activity indicators, they should question the customer on the reason for conducting the transaction(s) and the identity of the source

and ultimate beneficiary of the money being transacted. Staff should consider whether the customer's story amounts to a reasonable and legitimate explanation of the financial activity observed. If not, then the customer's activity should be regarded as suspicious and a suspicious transaction report should be made to the JFIU.

On occasions staff of insurance institutions may be reluctant to ask questions of the type mentioned above. Grounds for this reluctance are that the customer may realize that he, or she, is suspected of illegal activity, or regards such questions as none of the questioner's business. In either scenario the customer may be offended or become defensive and uncooperative, or even take his, or her, business elsewhere. This is a genuine concern but can be overcome by staff asking questions which are apparently in furtherance of promoting the services of the insurance institution or satisfying customer needs, but which will solicit replies to the questions above without putting the customer on his, or her, guard.

Appropriate questions to ask in order to obtain an explanation of the reason for conducting a transaction bearing suspicious activity indicators will depend upon the circumstances of the financial activity observed. For example, if a customer wishes to make a large cash transaction then staff can ask the customer the reason for using cash on the grounds that the staff may be able to offer advice on a more secure method to perform the transaction.

Persons engaged in legitimate business generally have no objection to, or hesitation in answering such questions. Persons involved in illegal activity are more likely to refuse to answer, give only a partial explanation or give an explanation which is unlikely to be true.

If a customer is unwilling, or refuses, to answer questions or gives replies which staff suspect are incorrect or untrue, this may be taken as a further indication of the suspicious nature of the financial activity.

Step three: **F**ind out the customer's records: Review of information already known when deciding if the apparently suspicious activity is to be expected

The third stage in the systemic approach to suspicious activity identification is to review the information already known to the insurance institution about the customer and his, or her, previous financial activity and consider this information to decide if the apparently suspicious activity is to be expected from the customer. This stage is commonly known as the "know your customer principle".

Insurance institutions hold various pieces of information on their customers which can be useful when considering if the customers'

financial activity is to be expected or is unusual. Examples of some of these information items and the conclusions which may be drawn from them are listed below:

(a) The customers' occupation. Certain occupations imply the customer is a low wage earner e.g. driver, hawker, waiter, student. The purchase of insurance policies with large transaction amounts from such customers would not therefore be expected.

(b) The customers' residential address. A residential address in low cost housing, e.g. public housing, may be indicative of a low wage earner.

Step four: **E**valuate all the above information: Is the transaction suspicious?

The final step in the suspicious activity identification system is the decision whether or not to make a STR. Due to the fact that suspicion is difficult to quantify, it is not possible to give exact guidelines on the circumstances in which a STR should, or should not, be made. However, such a decision will be of the highest quality when all the relevant circumstances are known to, and considered by, the decision maker, i.e. when all three of the preceding steps in the suspicious transaction identification system have been completed and are considered. If, having considered all the circumstances, staff find the activity genuinely suspicious then an STR should be made.

IMPORTANT NOTE

The above information is extracted from the relevant part of the website of the JFIU at ***http://www.jfiu.gov.hk/eng/suspicious_screen.html***. Insurance institutions are advised to regularly browse the website for latest information.

INDICATORS OF SUSPICIOUS TRANSACTIONS

1. A request by a customer to enter into an insurance contract(s) where the source of the funds is unclear or not consistent with the customer's apparent standing.

2. 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.

3. A proposal which has no discernible purpose and a reluctance to divulge a "need" for making the investment.

4. A proposal to purchase and settle by cash.

5. A proposal to purchase by utilizing a cheque drawn from an account other than the personal account of the proposer.

6. The prospective client who does not wish to know about investment performance but does enquire on the early cancellation/surrender of the particular contract.

7. A customer establishes a large insurance policy and within a short period of time cancels the policy, requests the return of the cash value payable to a third party.

8. Early termination of a product, especially in a loss.

9. A customer applies for an insurance policy relating to business outside the customer's normal pattern of business.

10. A customer requests for a purchase of insurance policy in an amount considered to be beyond his apparent need.

11. 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.

12. A customer refuses, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue.

13. 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 institution to verify.

14. Delay in the provision of information to enable verification to be completed.

15. Opening accounts with the customer's address outside the local service area.

16. Opening accounts with names similar to other established business entities.

17. Attempting to open or operating accounts under a false name.

18. Any transaction involving an undisclosed party.

19. A transfer of the benefit of a product to an apparently unrelated third party.

20. A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy).

21. Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policy holder.

22. The customer accepts very unfavourable conditions unrelated to his health or age.

23. An atypical incidence of pre-payment of insurance premiums.

24. Insurance premiums have been paid in one currency and requests for claims to be paid in another currency.

25. 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.)

26. 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.

27. A customer appears to have policies with several institutions.

28. A customer wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.

29. The customer who is based in jurisdictions which do not or insufficiently apply the FATF Recommendations designated by the FATF from time to time or in countries where the production of drugs or drug trafficking may be prevalent.

30. The customer who is introduced by an overseas agent, affiliator or other company that is based in jurisdictions which do not or insufficiently apply the FATF Recommendations designated by the FATF from time to time or in countries where corruption or the production of drugs or drug trafficking may be prevalent.

31. A customer who is based in Hong Kong and is seeking a lump sum investment and offers to pay by a wire transaction or foreign currency.

32. Unexpected changes in employee characteristics, e.g. lavish lifestyle or avoiding taking holidays.

33. Unexpected change in employee or agent performance, e.g. the sales person selling products has a remarkable or unexpected increase in performance.

34. Consistently high activity levels of single premium business far in excess of any average company expectation.

35. The use of an address which is not the client's permanent address, e.g. utilization of the salesman's office or home address for the despatch of customer documentation.

IMPORTANT NOTE

The IAIS has published relevant examples and indicators involving insurance in a document called "Examples of money laundering and suspicious transactions involving insurance". The document can be downloaded from IAIS website at ***http://www.iaisweb.org/__temp/Examples_of_money_laundering.pdf***. The list will be updated periodically to include additional examples identified. Insurance institutions are advised to regularly browse the website for latest information.

EXAMPLES OF MONEY LAUNDERING SCHEMES[18]

LIFE INSURANCE

Case 1

In 1990, a British insurance sales agent was convicted of violating a money laundering statute. The insurance agent was involved in a money laundering scheme in which over US$1.5 million was initially placed with a bank in England. The "layering process" involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent's supervisor was also charged with violating the money laundering statute. This case has shown how money laundering, coupled with a corrupt employee, can expose an insurance company to negative publicity and possible criminal liability.

Case 2

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

Case 3

Customs officials in Country X initiated an investigation which identified a narcotics trafficking organization utilized the insurance sector to launder proceeds. Investigative efforts by law enforcement agencies in several different countries

[18] Majority of the examples of money laundering schemes in this annex are extracted from the IAIS document "Examples of money laundering and suspicious transactions involving insurance". The document can be downloaded at ***http://www.iaisweb.org/__temp/Examples_of_money_laundering.pdf***.

identified narcotic traffickers were laundering funds through Insurance firm Z located in an off-shore jurisdiction.

Insurance firm Z offers investment products similar to mutual funds. The rate of return is tied to the major world stock market indices so the insurance policies were able to perform as investments. The account holders would over-fund the policy, moving monies into and out of the fund for the cost of the penalty for early withdrawal. The funds would then emerge as a wire transfer or cheque from an insurance company and the funds were apparently clean.

To date, this investigation has identified that over US$29 million was laundered through this scheme, of which over US$9 million has been seized. Additionally, based on joint investigative efforts by Country Y (the source country of the narcotics) and Country Z customs officials, several search warrants and arrest warrants were executed relating to money laundering activities involved individuals associated with Insurance firm Z.

Case 4

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

Case 5

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

Case 6

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

Case 7

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

Case 8

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

REINSURANCE

Case 1

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

INTERMEDIARIES

Case 1

A person (later arrested for drug trafficking) made a financial investment (life insurance) of US$250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of US$250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raise no suspicion at the

bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling US$250,000, thus avoiding the raising suspicions with the insurance company.

Case 2

Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing the due diligence checks.

The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses, but coming away with a clean cheque from the institution.

On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.

Case 3

An insurance company was established by a well-established insurance management operation. One of the clients, a Russian insurance company, had been introduced through the management of the company's London office via an intermediary.

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

Case 4

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 US$400,000 deposited with a life-insurer. The consulting company obtained powers of attorney for the account. Immediately following the setting up of the account, the consulting company withdrew the entire fee stipulated by the consulting contract. The insurer reported the transaction as suspicious. It turns out that an employee of the consulting company was involved in several similar cases. The account is frozen.

OTHER EXAMPLES

Single premiums

An example involves the purchase of large, single premium insurance policies and their subsequent rapid redemption. A money launderer does this to obtain payment from an insurance company. The person may face a redemption fee or cost, but this is willingly paid in exchange for the value that having funds with an insurance company as the immediate source provider.

In addition, the request for early encashment of single premium policies, for cash or settlement to an individual third party may arouse suspicion.

Return premiums

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

(a) a number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time;

(b) return premium being credited to an account different from the original account;

(c) requests for return premiums in currencies different from the original premium; and

(d) regular purchase and cancellation of policies.

Overpayment of premiums

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

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

- the overpayment is over a certain size (say US$10,000 or equivalent);
- the request to refund the excess premium was to a third party;
- the assured is in a jurisdiction associated with money laundering; and
- where the size or regularity of overpayments is suspicious.

High brokerage / third party payments / strange premium routes

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

Assignment of claims

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

IMPORTANT NOTE

Apart from the above examples of money laundering schemes, the FATF has also published annually detailed typologies involving insurance supported by useful case examples in documents called "Money Laundering & Terrorist Financing Typologies". The documents can be downloaded at the publications section of FATF website at ***http://www.fatf-gafi.org***. Insurance institutions are advised to regularly browse the website for latest information.

SAMPLE REPORT MADE TO THE JOINT FINANCIAL INTELLIGENCE UNIT

<table>
<tr><td colspan="4">Report made under section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance/Organized and Serious Crimes Ordinance or section 12 of the United Nations (Anti-Terrorism Measures) Ordinance to the Joint Financial Intelligence Unit</td><td colspan="2">Date :
Ref. No. :</td></tr>
<tr><td colspan="2">NAME AND ADDRESS OF INSURANCE INSTITUTION</td><td colspan="4"></td></tr>
<tr><td colspan="2">NAME OF SUSPICIOUS CUSTOMER (in full)</td><td colspan="4"></td></tr>
<tr><td colspan="2">DATE OF ISSUE OF INSURANCE POLICY (if applicable)</td><td></td><td colspan="2">DATE OF BIRTH / DATE OF INCORPORATION*</td><td></td></tr>
<tr><td colspan="2">OCCUPATION & EMPLOYER / NATURE OF BUSINESS*</td><td colspan="4"></td></tr>
<tr><td colspan="2">NATIONALITY / PLACE OF INCORPORATION*</td><td></td><td colspan="2">HKID / PASSPORT / BUSINESS REGISTRATION NO.*</td><td></td></tr>
<tr><td colspan="2">ADDRESS OF CUSTOMER</td><td colspan="4"></td></tr>
<tr><td>INFORMATION OF THE BENEFICIARY</td><td colspan="2">NAME & ADDRESS, RELATION WITH CUSTOMER</td><td>DATE OF BIRTH / DATE OF INCORPORATION*</td><td>HKID / PASSPORT NO.</td><td>NATIONALITY / PLACE OF INCORPORATION*</td></tr>
<tr><td colspan="2">DETAILS OF TRANSACTION AROUSING SUSPICION, AND THE SUM INVOLVED INDICATING SOURCE & CURRENCY USE. PLEASE ALSO ENCLOSE COPY OF THE TRANSACTION AND OTHER RELEVANT DOCUMENT</td><td>PARTICULARS OF TRANSACTION</td><td>AMOUNT</td><td>DATE</td><td>SOURCE</td></tr>
<tr><td colspan="2">OTHER RELEVANT INFORMATION INCLUDING REASON FOR SUSPICION AROUSED</td><td colspan="4"></td></tr>
<tr><td colspan="2">REPORTING OFFICER / TEL. NO.</td><td colspan="2">SIGNATURE</td><td colspan="2">ENTERED RECORDS</td></tr>
</table>

** in the case of a corporation*

JOINT FINANCIAL INTELLIGENCE UNIT CONTACT DETAILS

Written report should be sent to the Joint Financial Intelligence Unit at either the address, fax number, e-mail or PO Box listed below:

The Joint Financial Intelligence Unit,
28/F, Arsenal House West Wing,
Hong Kong Police Headquarters,
Arsenal Street,
Hong Kong.

or

The Joint Financial Intelligence Unit,
GPO Box 6555,
Hong Kong Post Office,
Hong Kong.

Tel: 2866 3366

Fax: 2529 4013

Email: jfiu@police.gov.hk

Urgent reports should be made either by fax, e-mail or by telephone to 2866 3366.

SAMPLE ACKNOWLEDGEMENT LETTER ISSUED BY THE JOINT FINANCIAL INTELLIGENCE UNIT

Date:

The Compliance Officer
Any Insurance Co./Broker

Your ref.:

Dear Sir,

Drug Trafficking (Recovery of Proceeds) Ordinance
Organized and Serious Crimes Ordinance
United Nations (Anti-Terrorism Measures) Ordinance

I refer to your disclosure made to the Joint Financial Intelligence Unit on [ ] under the above references.

I acknowledge receipt of the information supplied by you under the provisions of Section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 and the Organized and Serious Crimes Ordinance, Cap. 455 / Section 12 of the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575.

Based upon the information currently available, consent is given for you to continue to operate the account(s) in accordance with normal insurance practice under the provisions of the Ordinance(s).

Thank you for your co-operation.

Yours faithfully,

Joint Financial Intelligence Unit