27th April 2016

NOTICE

ANNEX II – Sector Specific Guidance Notes for Anti-Money Laundering & Anti-Terrorist Financing (AML/ATF) Regulated Financial Institutions carrying out Long-Term insurance business

BACKGROUND

The Bermuda Monetary Authority (the Authority) has undertaken a review of the Guidance Notes for Anti-Money Laundering and Anti-Terrorism Financing (AML/ATF GN) to ensure compliance with the revised 40 recommendations that were published in 2012 by the Financial Action Task Force (FATF). The Authority issued the AML/ATF GN for consultation and is currently reviewing the comments received from stakeholders.

The Authority will be issuing a series of sector-specific guidance that will accompany the AML/ATF GN which is intended to apply the AML/ATF GN to the nature and risk profile of the specific sector. These sector-specific guidance notes supplement, and must be read in conjunction with the AML/ATF GN. The sector-specific guidance notes do not replace the AML/ATF GN.

CONSULTATION

The Authority is inviting comments from all stakeholders on the "Sector-Specific AML/ATF Guidance Notes for Long-Term insurance business".

The consultation period is 30 days and ends on 27th May 2016.

Comments should be sent to policy@bma.bm and include the words "AML/ATF Long-Term insurance business" in the subject of the e-mail.

ANNEX II

Sector-Specific Guidance Notes for Long-Term Insurance Business

These sector-specific guidance notes should be read in conjunction with the main guidance notes for AML/ATF regulated financial institutions on anti-money laundering and anti-terrorism financing.

ANNEX II - SECTOR-SPECIFIC GUIDANCE NOTES FOR LONG-TERM INSURANCE BUSINESS

Table of Contents

ANNEX II - SECTOR-SPECIFIC GUIDANCE NOTES FOR LONG-TERM INSURANCE BUSINESS

Introduction

II.1 This annex sets forth guidance on AML/ATF obligations under the Acts and Regulations of Bermuda that are specific to Long-Term insurance business.

II.2 Under Regulation 2(2)(c) and (d) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (the Regulations), a person is designated as an anti-money laundering and anti-terrorist financing (AML/ATF) regulated financial institution (RFI) if the person is:

- An insurer (and not a reinsurer) registered under Section 4 of the Insurance Act 1978; or
- An insurance manager or broker registered under Section 10 of the Insurance Act 1978

and the person carries on or acts in connection with Long-Term business (other than reinsurance business) falling within paragraph (a) or (c) of the definition of "long-term business" in section 1(1) of the Insurance Act 1978.

II.3 The Long-Term business described in section 1(1)(a) and (c) of the Insurance Act 1978 includes:

- Effecting and carrying out contracts of insurance on human life or contracts to pay annuities on human life; and
- Effecting and carrying out contracts of insurance, whether effected by the issue of policies, bonds or endowment certificates or otherwise, whereby in return for one or more premiums paid to the insurer a sum or a series of sums is to become payable to the persons insured in the future, not being contracts associated with life insurance, annuities, injury due to accident or incapacitation, or dying in consequence of disease.

II.4 All RFIs must comply with the Acts and Regulations, and with the main AML/ATF guidance notes issued by the Bermuda Monetary Authority (Authority or BMA).

II.5 RFIs conducting insurance business should read these sector specific guidance notes in conjunction with the main guidance notes for AML/ATF regulated financial institutions on anti-money laundering and anti-terrorist financing. This annex supplements, but does not replace the main guidance notes.

II.6 Portions of this annex summarise or cross-reference relevant information that is contained in detail in the main guidance notes. The detailed information in the main guidance notes remains the authoritative guidance.

II.7 Portions of this annex include sector-specific information, such as risk indicators that are particular to insurance business. This sector-specific information should be considered as supplementary to the main guidance notes.

Status of the guidance

II.8 Approved by the Minister of Justice, these guidance notes are issued by the Authority under Section 5(2) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (SEA Act 2008), Section 49A of the Proceeds of Crime Act 1997 (POCA 1997), and Section 12B of the Anti-Terrorism (Financial and Other Measures) Act 2004 (ATFA 2004).

II.9 These guidance notes are of direct relevance to all senior management, inclusive of the Compliance Officer, and to the Reporting Officer. The primary purpose of the notes is to provide guidance to those who set the RFI's risk management policies, procedures and controls for the prevention and detection of money laundering and terrorist financing (ML/TF).

II.10 The Court, or the Authority, as the case may be, in determining whether a person is in breach of a relevant provision of the Acts or Regulations, is required to consider whether a person has followed any relevant guidance approved by the Minister of Justice and issued by the Authority. These requirements upon the Court or Authority are detailed in the provisions of Section 49M of POCA 1997, Regulation 19(2), Section 12(O) of, and paragraph 1(6) of Part I, Schedule I to, ATFA 2004 and Section 20(6) of the SEA Act 2008.

II.11 When a provision of the Acts or Regulations is directly described in the text of the guidance, the guidance notes use the term **"must"** to indicate that the provision is mandatory.

II.12 In other cases, the guidance uses the term **"should"** to indicate ways in which the requirements of the Acts or Regulations may be satisfied, while allowing for alternative means, provided that those alternatives effectively accomplish the same objectives.

II.13 Departures from this guidance, and the rationale for so doing, should be documented, and RFIs should stand prepared to justify departures to authorities such as the BMA.

II.14 RFIs should be aware that under Section 16 of the Financial Intelligence Agency Act 2007, the Financial Intelligence Agency (FIA) may, in the course of enquiring into a suspicious transaction or activity relating to money laundering or terrorist financing, serve a notice in writing on any person requiring the person to provide the FIA with such information as it may reasonably require for the purpose of its enquiry.

II.15 Detailed information is set forth in the main guidance notes, beginning with the Preface.

Senior management responsibilities and internal controls

II.16 The AML/ATF responsibilities for senior management of an RFI conducting insurance business are governed primarily by POCA 1997, SEA Act 2008, ATFA 2004, and Regulations 16, 17 and 19.

II.17 The AML/ATF internal control requirements for RFIs conducting insurance business are governed primarily by Regulations 12, 16 and 18.

II.18 Regulation 19 provides that failure to comply with the requirements of specified Regulations is a criminal offence and carries with it significant penalties. On summary conviction, the penalty is a fine of up to $50,000. Where conviction occurs on indictment, penalties include a fine of up to $750,000, imprisonment for a term of two years, or both.

II.19 Section 20 of the SEA Act 2008 empowers the Authority to impose a penalty on an RFI of up to $500,000 for each failure to comply with specified Regulations. The SEA Act also provides for a number of criminal offences, including carrying on business without being registered pursuant to Section 33 of the SEA Act.

II.20 Under the Acts and Regulations of Bermuda, senior management in all RFIs must:

- Ensure compliance with the Acts and Regulations;
- Identify, assess and effectively mitigate the ML/TF risks the RFI faces amongst its customers, products, services, transactions, delivery channels, outsourcing arrangements and geographic connections;
- Ensure that risk assessment findings are maintained up to date;
- Appoint a Compliance Officer at the senior management level to oversee the establishment, maintenance and effectiveness of the RFI's AML/ATF policies, procedures and controls;
- Appoint a Reporting Officer to process disclosures to the FIA;
- Screen employees against high standards;

- Ensure that adequate resources are devoted to the RFI's AML/ATF policies, procedures and controls;
- Audit and periodically test the RFI's AML/ATF policies, procedures and controls for effectiveness; and
- Recognise potential personal liability if legal obligations are not met.

II.21 RFIs must establish and maintain detailed policies, procedures and controls that are adequate and appropriate to forestall and prevent operations related to ML/TF.

II.22 Where a Bermuda RFI conducting insurance business has branches, subsidiaries or representative offices located in a country or territory other than Bermuda, it must communicate its AML/ATF policies and procedures to all such entities and must ensure that all such entities apply AML/ATF measures at least equivalent to those set out in the Acts and Regulations.

II.23 Attempts to launder money through an insurance company may be carried out in any one or several of three ways:

- Internally, by a director, manager or employee, either individually or in collusion with others inside and/or outside of the company;
- Externally, by a policyholder seeking to place illicit funds with an insurance company for subsequent recovery; and
- Indirectly, by a third party service provider or by an insurance agent, broker, manager, or other intermediary facilitating the placement of illicit funds on behalf of either a policyholder or a third party or intermediary itself.

II.24 The majority of this annex addresses attempted money laundering by policyholders. Money laundering risks involving intermediaries and third party service providers are addressed in paragraphs II.35 through II.38. Money laundering risks involving internal directors, managers or employees, however, are addressed in paragraphs II.39 through II.42.

II.25 Specific requirements for an RFI's detailed policies, procedures and controls are set forth in chapters 2 through 11 of the main guidance notes.

II.26 Additional details are set forth in Chapter 1: Senior Management Responsibilities and Internal Controls.

<u>Links between insurance business practices and AML/ATF policies, procedures and controls</u>

II.27 Persons carrying on all types of insurance business generally engage in business processes that achieve many of the objectives of the AML/ATF policies, procedures and controls required by the Acts and Regulations. These business processes include:

- The underwriting process through which a customer profile is established and financial risks to the insurer are identified and assessed in order to set an adequate premium;
- The maintenance and monitoring of a customer's profile and transactions for purposes of active client management;
- The claims process through which the circumstances and veracity of a policyholder's claim are evaluated; and
- Processes to guard against fraud and reputational, operational and legal risk.

II.28 These business processes provide a suitable foundation for the AML/ATF policies, procedures and controls required by the Acts and Regulations. An RFI should not presume, however, that its existing processes are sufficient. Each RFI must ensure that it meets each of the AML/ATF obligations under the Bermuda Acts, Regulations and these guidance notes, whether as part of its existing business processes or through separate processes.

II.29 Persons carrying on insurance business often check applicants, their beneficial owners and beneficiaries against internal and external information to evaluate insurance risks and to identify known fraudsters. Similarly, customers, beneficial owners and beneficiaries should also be checked against internal and external information to identify known criminals, politically exposed persons (PEPs) and targets of domestic and international sanctions.

II.30 Criminals who launder money through insurance companies are attracted primarily by the good reputation that many insurance companies enjoy and the ability to place illicit funds in an insurance product for later withdrawal. An insurance company's good reputation is both attractive to money launderers, and at risk in the event that money laundering occurs.

II.31 Although criminals may lose a portion of the funds invested in an insurance product, for example due to early withdrawal fees, criminals are willing to accept financial losses as the cost of obtaining from a reputable insurance company funds that appear to be legitimate and which are therefore less likely to trigger suspicion in the receiving institution.

II.32 Persons carrying on insurance business should focus not only on potential fraud against the insurance company, but also on preventing crime, by understanding the ownership and origin of any funds used to remit an insurance premium or any other payment connected with an insurance product.

II.33 Each person carrying on insurance business should record in detail the basis on which each applicant has been accepted. Decisions to enter into business relationships with identified high risk customers, such as Foreign PEPs, must be taken exclusively at the senior management level. See paragraphs 5.97 through 5.117 of the main guidance notes.

II.34 Persons carrying on insurance business should also ensure that knowledge, suspicion, and reasonable grounds to know or suspect that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing, are reported to the FIA.

Intermediaries and third party service providers

II.35 The ML/TF risks associated with insurance business are increased by the reliance of many insurance companies on agents, brokers, introducers, managers, and other intermediaries to interact with insurance applicants, policyholders, controllers and beneficiaries.

II.36 Where an intermediary is not acting directly under the control or supervision of the insurer, there is a heightened inherent risk that the intermediary is unaware of, or unwilling to conform to, required AML/ATF policies, procedures and controls. In turn, there is a heightened inherent risk that the intermediary will fail to apply appropriate due diligence measures on the customer and source of funds and will fail to recognise and report knowledge, suspicion, and reasonable grounds to know or suspect that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing.

II.37 The use of third party service providers to apply customer due diligence (CDD) and other measures similarly heightens the inherent risk of an AML/ATF failure.

II.38 To ensure that intermediaries and third party service providers are applying appropriate AML/ATF measures and are providing insurers with suitable and adequate documentation, insurers must carefully apply appropriate reliance and outsourcing measures. See paragraphs II.108 through II.128, 3.23 through 3.24, 5.118 through 5.148 and 5.149 through 5.178 (of the main guidance notes).

Ownership, management and employee checks

II.39 To guard against potential money laundering involving owners, directors, managers and employees, insurers should screen such persons against high standards in accordance with paragraphs 1.70 through 1.74 of the main guidance notes.

II.40 RFIs should ensure that screenings are conducted both for the RFI itself and for any third party service provider, reinsurer, agent, broker, introducer, manager, or other intermediary.

II.41 Where any screening is conducted by a third party, the RFI should have procedures to satisfy itself as to the effectiveness of the screening procedures the third party uses to ensure the competence and probity of each owner, director, manager and employee subject to screening.

II.42 Working with insurers, reinsurers, intermediaries and third party service providers that apply AML/ATF measures at least equivalent to those in Bermuda is likely to reduce the measures a Bermuda RFI will need to undertake in order to meet its screening obligations.

Risk-based approach for RFIs conducting insurance business

II.43 RFIs conducting insurance business must employ a risk-based approach in determining:

- Appropriate levels of CDD measures;
- Proportionate risk-mitigation measures to prevent the abuse of the RFI's products, services and delivery channels for ML/FT purposes;
- The level of reliance, if any, that can reasonably be placed upon an insurance agent, broker, manager, or other intermediary;
- The scope and frequency of ongoing monitoring; and
- Measures for detecting and reporting suspicious activity.

II.44 The purpose of an RFI applying a risk-based approach is to balance the cost of AML/ATF compliance resources with a realistic assessment of the risk of the RFI being used in connection with ML/TF. A risk-based approach focuses resources and efforts where they are needed and where they have the greatest impact in preventing and suppressing ML/TF.

II.45 The higher the ML/TF risk an RFI faces from any particular combination of customer, product, service, transaction, delivery channel or geographic connection, the stronger and/or more numerous the RFI's mitigation measures must be.

II.46 Although RFIs conducting insurance business should target compliance resources toward higher-risk situations, they must also continue to apply risk mitigation measures to any standard- and lower-risk situations, commensurate with the risks identified. The fact that a customer or transaction is assessed as being lower risk does not mean the customer or transaction is not involved in ML/TF.

II.47 RFIs should document and be in a position to justify the basis on which they have assessed the level of risk associated with each particular combination of customer, product, service, transaction, delivery channel or geographic connection.

II.48 When designing a new product, an RFI conducting insurance business must assess the risk of the product being used for ML/FT.

II.49 Detailed information on the requirement that RFIs use a risk-based approach to mitigate the risks of being used in connection with ML/TF is set forth in Chapter 2: Risk-Based Approach.

ML/TF risks in long-term insurance business

II.50 Using the risk-based approach, each RFI conducting insurance business should determine the amount of ML/TF risk it will accept in pursuit of its business goals.

II.51 Nothing in the Acts or Regulations prevents an RFI from deliberately choosing to accept higher-risk insurance business. Each RFI must, however, ensure that it has the capacity and expertise to apply risk mitigation measures that are commensurate with the risks it faces, and that it does effectively apply those measures.

II.52 Generally, the level of risk associated with insurance business is highest for life insurance and annuity products. Other insurance products, however, while generally not providing sufficient functionality and flexibility to be a primary choice for ML/TF, can and have been abused for money laundering and terrorist financing purposes.

II.53 Although the Acts and Regulations do not create AML/ATF obligations for all types of insurance, ML/TF risks or suspicions may arise outside of the context of life insurance, annuities, or other forms of Long-Term business. Although the Acts and Regulations do not create AML/ATF obligations for all types of insurance, money laundering/terrorist financing risks or suspicions may arise outside of the context of life insurance, annuities, or other forms of Long-Term business. Sections 46(A1) and 46(1) of the POCA require

persons to report knowledge or suspicion of money laundering to the FIA. This requirement applies to all persons, whether or not they meet the definition of a RFI.

II.54 As a general matter, a non-exhaustive list of factors that will affect the level of risk of any insurance transaction or business relationship includes:

- The applicant for business, and any beneficial owner;
- The beneficiaries:
- The product to be underwritten or sold;
- The involvement of any intermediaries or third party service providers;
- The nature of the business relationship formed;
- Geographic connections;
- The methods used to send and receive any payment connected with the product; and
- Transactions undertaken following the establishment of the business relationship.

II.55 Although risks may arise in a number of ways, RFIs conducting insurance business should take particular note of the heightened ML/TF risks associated with the following insurance arrangements:

- Single premium life insurance policies that store value;
- Investment-linked or other single premium contracts that store value;
- Fixed and variable annuities; and
- Endowment (second hand) policies.

II.56 Additional indicators of higher risk in insurance business are discussed in detail in paragraphs II.222 through II.238.

Customer due diligence

II.57 RFIs conducting insurance business must carry out CDD.

II.58 Detailed information on CDD is set forth in chapters 3, 4, and 5 of the main guidance notes, and paragraphs II.57 through II.190.

II.59 RFIs must know the identities of their insurance customers, their customers' sources of funds and wealth, and the purpose and intended nature of their insurance customers' activities.

II.60 CDD information assists RFIs in knowing who the customer is, understanding the true source of funds flowing through the insurance product, and establishing norms for expected customer profiles and conduct.

II.61 Carrying out CDD also allows RFIs to:

- Guard against impersonation and other fraud by being satisfied that customers are who they say they are;
- Know whether a customer is acting on behalf of another;
- Identify any legal barriers (e.g. international sanctions) to providing the product or service requested;
- Maintain a sound basis for identifying, limiting and controlling risk exposure;
- Avoid committing offences under POCA and ATFA relating to ML/TF; and
- Assist law enforcement by providing information on insurance customers or activities being investigated.

II.62 CDD measures that must be carried out include:

- Understanding the purpose and intended nature of the customer's business relationship with the RFI;
- Identifying the source of wealth and source of funds associated with the customer;
- Identifying and verifying the identity of each customer;
- Identifying and taking reasonable measures to verify the identity of the beneficial owner(s) of the customer;
- Identifying and verifying the identity of the beneficiary of the insurance product; and
- Updating the CDD information at appropriate times.

II.63 High-level principles regarding CDD are set forth in Chapter 3: Overview of Customer Due Diligence.

<u>Purpose and intended nature of the customer's business relationship with the RFI</u>

II.64 An RFI must understand the purpose and intended nature of each proposed business relationship or transaction. In some instances the purpose and intended nature of a proposed business relationship may appear self-evident. Nonetheless, an RFI must obtain information that enables it to document and categorise the nature, purpose, size and complexity of the business relationship, such that it can be effectively monitored.

II.65 To obtain an understanding sufficient to monitor an insurance business relationship or transaction, an RFI should collect information, including, but not limited to:

- The nature and intended purpose of the insurance product;
- The source of wealth and source of funds to be used in the insurance business relationship;
- The anticipated type, volume, value, frequency and nature of the activity that is likely to be undertaken through the insurance business relationship;
- The geographic connections of the applicant, beneficial owner, beneficiary and any controller;
- The means of payment (cash, wire transfer, other means of payment);
- Whether there is any bearer arrangement, and if so, the reasons for and details of the arrangement; and
- Whether any payments are to be made to or by third parties, and if so, the reasons for and details of the request.

Source of wealth and source of funds

II.66 Enquiries regarding the source of wealth and source of funds are among the most useful sources of information leading to knowledge, suspicion, or reasonable grounds to know or suspect that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing.

II.67 RFIs should make enquiries as to how a customer has acquired the wealth to be used as a premium for, or contribution to, an insurance policy.

II.68 The extent of such enquiries should be made using a risk-based approach.

II.69 RFIs should also ensure that they understand the source of funds and specific means of payment, including the details of any account, which a customer proposes to use. See paragraphs II.134 through II.144.

II.70 Additional information on source of funds and source of wealth is set forth in paragraphs 5.110 through 5.113 of the main guidance notes.

Definition of customer in an insurance business context

II.71 An RFI's customer is generally the private individual or individuals with and for whom a business relationship is established, or with or for whom an occasional transaction is carried out. A given insurance arrangement may have more than one private individual that is a customer, whether directly or as a beneficial owner, director, manager or employee of a legal person, trust or other legal arrangement.

II.72 For the purposes of the Acts, Regulations and these guidance notes, a customer includes each of the following:

- Any private individual, legal person, trust, or other legal arrangement that is an **applicant** for, or **policyholder** of, an insurance product;
- Any **beneficial owner** of an applicant or policyholder;
- Any **beneficiary** or other person on whose behalf an applicant or policyholder is acting; and
- Any private individual, legal person, trust, or other legal arrangement, and any beneficial owner thereof, that is a **controller** able to exercise significant power over the insurance product.

II.73 Full information on the meaning of customer, business relationship and occasional transaction, and on identifying and verifying individuals, legal persons, trusts and other legal arrangements is set forth in Chapter 4: Standard Customer Due Diligence Measures.

Identifying and verifying insurance customers

II.74 In line with the main guidance notes for private individuals and legal persons contained in Chapter 4, Standard Customer Due Diligence Measures, RFIs must obtain and verify identification information for each person who is a customer in the insurance business context.

Obtaining and verifying insurance applicant identification information

II.75 A person who is an applicant in the insurance business context may be a private individual, legal person, trust, or other legal arrangement. For each type of applicant, an RFI should follow the identification and verification requirements in Chapter 4: Standard Customer Due Diligence Measures.

II.76 Where an applicant is a legal person, trust or other legal arrangement, the RFI should obtain and verify the identity of each private individual owning or acting on behalf of the legal person, trust or other legal arrangement, and should ascertain whether such person is appropriately authorised.

II.77 Where the applicant is a company or organisation applying for group insurance coverage on behalf of its staff, employees or members, the RFI should obtain and verify the identity of the applicant company or organisation as a set out in Chapter 4: Standard Customer Due Diligence Measures and, where relevant, Chapter 5: Non-Standard

Customer Due Diligence Measures. RFIs should maintain a list of all participants in the group plan and should review and update the list using a risk-based approach.

II.78 Verification of identity must be completed for each applicant, beneficiary or third party receiving any payment, prior to the payment's initiation.

Obtaining and verifying beneficial owner information

II.79 In addition, and in line with the guidance for private individuals, legal persons, trusts, and other legal arrangements, RFIs must obtain and verify identification information for the beneficial owners of any applicant.

II.80 RFIs should bear in mind that, in contrast to insurance business where a beneficial owner of an applicant and a beneficiary may be different persons, within the context of a trust, a beneficial owner and beneficiary are often the same person.

II.81 Information on the identification and verification of beneficial owners is set forth in Regulation 3 and Chapter 4: Standard Customer Due Diligence Measures.

II.82 Additional information specific to the beneficial ownership of trusts is set forth in Regulation 3(3) and paragraphs I.78 through I.87.

Obtaining and verifying beneficiary information

II.83 In line with the guidance for private individuals and legal persons, RFIs must obtain and verify identification information for all known beneficiaries of an insurance product.

II.84 A beneficiary is known if the applicant, any authorised representative thereof, or any controller has named the beneficiary.

II.85 Often, a beneficiary will be a private individual, legal person, trust or other legal arrangement. Information on the identification and verification of such persons is set forth in Chapter 4: Standard Customer Due Diligence Measures and, as regards the beneficial owners of a trust, paragraphs I.78 through I.87.

II.86 Where the beneficiaries of an insurance product are one or more classes, RFIs must take reasonable steps to ascertain the identity of the members of each class or each part of a class that is most likely to receive a payment or exercise another vested right under the insurance policy in the foreseeable future.

II.87 The class most likely to receive a payment or exercise another vested right under the insurance policy is often termed the "primary" class. A class that is less likely, or less immediately, to receive a payment or exercise another vested right is often termed a "secondary," "tertiary" or "contingent" class.

II.88 Where the beneficiaries of an insurance policy are a primary class, for example, the children of X, there is only one class for which an RFI must obtain and verify identity. The RFI must:

- Identify the children of X; and
- Subsequently verify the identity of the children of X prior to allowing the exercise of any vested right.

II.89 Where the beneficiaries of an insurance product are both primary and contingent classes, for example, the adult children of X, and after their deaths, the adult grandchildren of X, and after their deaths, a charity, the adult children of X are the class most likely to receive a payment or exercise another vested right in the foreseeable future. The RFI must:

- Identify the children of X; and
- Subsequently verify the identity of each member of each class prior to allowing the exercise of any vested right.

II.90 Further information on the timing of verification of a beneficiary's identity is set forth in paragraphs II.102 through II.105.

<u>Obtaining and verifying controller information</u>

II.91 Where an applicant or policyholder has a controller, other than the applicant or policyholder and the beneficiaries, who is able to exercise significant power over the insurance policy, an RFI must identify and apply risk-based measures to verify the identity of the controller in line with the guidance for private individuals, legal persons, trusts and other legal arrangements.

II.92 Persons who may be controllers include, but are not limited to:

- Trustees;
- Nominees;
- Investment advisors; and
- Holders of a power of attorney or other third party mandate.

II.93 Where an RFI is reasonably satisfied that a controller is a regulated investment advisor subject to AML/ATF regulations at least equivalent to those in Bermuda, the RFI must fully identify the advisor, but may consider reducing the level of verification checks it carries out.

II.94 The RFI must record in its policyholder file the basis upon which the controller has been accepted as a regulated investment advisor. Where a regulated investment advisor acting as a controller ceases to be a regulated investment advisor, the RFI must verify the identity of the controller in line with the guidance for private individuals, legal persons, trusts and other legal arrangements.

II.95 For all controllers, regardless of whether the controller is a regulated investment advisor, the RFI should ensure that, in the case of a legal entity or arrangement, the individuals within the controller from whom the RFI is to receive instructions have been fully identified.

Timing of customer due diligence

II.96 An RFI must apply CDD measures when it:

- Establishes a business relationship;
- Carries out an occasional transaction in an amount of $15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked, or carries out any wire transfer in an amount of $1,000 or more (see Chapter 8: Wire Transfers);
- Suspects money laundering or terrorist financing; or
- Doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

II.97 RFIs conducting insurance business must identify the following before entering into any insurance contract:

- The applicant and any beneficial owners of the applicant;
- Any controllers;
- The purpose and intended nature of the business relationship; and
- The source of funds.

II.98 Before concluding any insurance contract, RFIs must also verify the identity of:

- The applicant;

- Any beneficial owners of the applicant; and
- Any controllers, subject to the exception set forth in paragraphs II.93 through II.94.

II.99 In addition, each time a sizeable accelerated payment or overpayment of premium is made, an RFI should obtain and verify the source of the funds and the objectives of the applicant.

II.100 Verification of identity should also take place, or be confirmed:

- Before any payment is made from the insurance product;
- Before allowing the exercise of any other vested right;
- Before any new controller is permitted to exercise significant power;
- Subsequently when there is any change in information previously provided; and
- When otherwise deemed necessary due to information obtained through risk-assessment or ongoing monitoring.

II.101 The identity of each beneficiary should normally be obtained at the outset of the business relationship. Where an insurance contract permits an applicant to delay naming a beneficiary, or permits changes to beneficiaries during the life of the insurance policy, the identity of the beneficiary may be obtained at the time the beneficiary is named.

II.102 Where the ML/TF risks are assessed as standard or lower than standard, and appropriate risk-mitigation measures are applied, verification of a beneficiary's identity may take place:

- At or before the time of any payout or premium refund; and
- At or before the time the beneficiary exercises any vested right under the policy.

II.103 Nonetheless, RFIs should ensure that their policies, procedures and controls do not categorically preclude the verification of a beneficiary's identity prior to a payout, refund or other exercise of a vested right. Instead, RFIs should ensure that the timing and extent of verification of a beneficiary's identity is conducted using a risk-based approach.

II.104 Where a particular insurance business relationship presents higher ML/TF risks, for example, where a PEP or target of international sanctions is involved, RFIs should verify all persons forming the relationship, including beneficiaries, to dispel or confirm any concerns.

II.105 At all times, verification of a beneficiary's identity must take place as soon as is practicable where:

- A beneficiary is the applicant, policyholder, beneficial owner of the applicant or policyholder, or controller; or
- A beneficiary is otherwise able to exercise significant power over assets held in the insurance product prior to the formal transfer of the assets into the beneficiary's ownership.

II.106 In order to keep aging identity information accurate and up-to-date, RFIs should take advantage of opportunities to obtain updated documentation. Such opportunities include, but are not limited to:

- A change in the address of an applicant, policyholder, controller or beneficiary;
- The appointment of a new controller;
- The expiration of a document establishing identity;
- Changes to named beneficiaries; and
- A receipt of payment from, or a request for payment to, a previously unknown account.

II.107 Detailed information on the timing of CDD measures is set forth in Chapter 3: Overview of Customer Due Diligence.

Reliance on intermediaries

II.108 As noted in paragraphs II.35 through II.38 the significant involvement of intermediaries in the insurance business requires RFIs to carefully implement reliance controls.

II.109 An RFI may choose to rely upon another person to apply certain CDD measures, provided that both the person being relied upon and the nature of the reliance meet certain criteria. In any reliance situation, however, the relying RFI retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

II.110 The CDD measures that an RFI may rely upon a person to apply are:

- Identifying and verifying the identity of the applicant, the applicant's beneficial owner, and any controllers;
- Identifying and verifying the beneficiary or beneficiaries;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship, including the source of wealth and source of funds.

II.111 In any reliance situation, the following duties remain with the relying RFI and cannot be delegated:

- Conducting ongoing monitoring to scrutinise transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the RFI's knowledge of the customer, beneficial owner, purpose and intended nature of the business relationship and, where necessary, the source of funds or wealth; and
- Reporting knowledge or suspicion of money laundering or terrorist financing.

II.112 However, within the limitations established by Act, Regulation and these guidance notes, intermediaries being relied upon may support an RFI in carrying out the duties described in paragraph II.111.

II.113 RFIs may rely upon a person who is:

For Bermuda persons

- An AML/ATF regulated financial institution under Section 2(2) of the Regulations; or
- A specified business under Section 3 of the Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008; or
- An independent professional as defined at Section (2)(1) of the Regulations; and
- Regulated, supervised or monitored for, and has measures in place for compliance with the AML/ATF Regulations of Bermuda.

<u>For non-Bermuda persons</u>

- An institution that carries on business corresponding to the business of an AML/ATF regulated financial institution or independent professional; and
- Regulated, supervised or monitored for, and has measures in place for compliance with AML/ATF regulations at least equivalent to those of Bermuda.

II.114 An RFI may rely upon another person or institution to carry out CDD measures only where:

- The RFI utilises a risk-based approach to determine the level of reliance it can reasonably place on an intermediary and the verification work the intermediary has carried out, and as a consequence, the amount of evidence that should be obtained directly from the customer.
- The intermediary being relied upon consents to being relied upon;

- The intermediary being relied upon confirms in writing that it has applied the CDD measures itself; and
- The intermediary being relied upon has carried out at least the standard level of customer verification.

II.115 Regardless of such reliance, Regulation 14(1)(b)(i) requires that RFIs must ensure and be satisfied that appropriate CDD must be done. Relying RFIs must satisfy themselves that copies of documents, data and other information used by the intermediary for verification of identity, purpose and intended nature of the business relationship, and the sources of wealth and funds will be made available by the intermediary upon request, without delay, for at least five years following the date on which the business relationship ends.

II.116 Periodically, and on a risk-sensitive basis, relying RFIs should test the willingness and ability of relied upon intermediaries to actually make available requested evidence of verification. This is particularly relevant when a customer is assessed as being higher risk, when the intermediary is situated in, or a transaction involves, a higher-risk jurisdiction, or when knowledge or suspicion of money laundering or terrorism financing is present.

II.117 In addition to using a risk-based approach to determine the level of reliance an RFI can place on an intermediary, RFIs should consider whether to introduce AML/ATF standards and related training as a condition of accepting or maintaining business from an intermediary.

II.118 Where an RFI has reason to believe that an intermediary is subject to insufficient or no legislation, regulation or guidance in respect of AML/ATF, or simply as a matter of good practice, the insurer should introduce measures to ensure that the intermediary has in place adequate policies, procedures and controls. These measures may include, but are not limited to:

- Requiring sight of the intermediary's AML/ATF policies, procedures and controls;
- Requesting and reviewing a copy of the relevant section of the last inspection report undertaken by the intermediary's regulator;
- Devising a standard set of customer due diligence procedures and requiring an undertaking from the intermediary that procedures to the same standard will be applied; and/or
- Requiring the right to physically audit the introducer's AML/ATF policies, procedures and controls, and periodically testing those policies, procedures and controls.

II.119 Any use of a pro-forma certificate should not unthinkingly be accepted as an adequate performance of CDD. Pro-forma certificates may reduce duplication of effort and documentation only where the RFI determines after careful assessment that the pro-forma certificate in combination with the RFI's and intermediary's AML/ATF policies, procedures and controls meets all of the requirements of the relevant Bermuda Acts, Regulations and guidance notes.

II.120 Paragraphs 5.118 through 5.148 (of the main guidance notes) set forth the circumstances in which reliance on an intermediary or other person is permissible. Paragraphs 3.22 through 3.24 (of the main guidance notes) provide additional relevant guidance. In any reliance situation, however, the relying RFI retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

II.121 Where an RFI determines that the information it has received is adequate, and all other criteria for relying upon an intermediary or other third party have been met, the RFI may determine that it has satisfied its CDD obligations.

II.122 Where, however, an RFI determines that relevant documentation is not available, or is inadequate, the RFI will need to obtain additional documentation, by ensuring that either:

- The relied upon intermediary obtains the information in accordance with the relevant Bermuda Acts, Regulations and guidance notes; or
- The relying RFI obtains the information itself.

Outsourcing

II.123 An outsourcing arrangement occurs where an RFI uses a service provider to perform an activity, such as applying CDD measures that would normally be carried out by the RFI. Irrespective of whether the service provider is in Bermuda or overseas, and irrespective of whether the service provider is within or independent of any financial sector group of which the RFI may be a member, any outsourcing arrangement is subject to the Regulations and these guidance notes.

II.124 Outsourced activities should be carried out in accordance with the RFI's procedures and the RFI should have effective control over the service provider's implementation of those procedures. An RFI's board or similarly empowered body or individual, such as the Compliance Officer, should establish clear accountability for all outsourced activities, as if the activities were performed in-house according to the RFI's own standards of internal control and oversight.

II.125 RFIs considering an outsourcing arrangement should carry out due diligence as to the service provider under consideration. The purpose of the due diligence is to determine whether the service provider has the ability, capacity, and any required authorisation to perform the outsourced activities reliably, professionally, and in accordance with the Regulations and these guidance notes. RFIs should establish a written policy concerning the scope and frequency of initial and ongoing due diligence carried out as to such service providers.

II.126 Where an RFI outsources any functions, including those carried out by insurance managers or contract employees, the RFI retains the ultimate responsibility to ensure that the activities or work carried out on its behalf are completed in accordance with the relevant Bermuda Acts, Regulations and guidance notes.

II.127 In any outsourcing arrangement, an RFI cannot contract out of its statutory and regulatory responsibilities to prevent and detect ML/TF.

II.128 Paragraphs 5.149 through 5.178 (of the main guidance notes) set forth the circumstances in which an outsourcing arrangement is permissible.

Refusing or terminating insurance business

II.129 If for any reason an RFI is unable to apply required CDD measures in relation to the applicant, policyholder, beneficial owner of the applicant or policyholder, controller, or beneficiary, Regulation 9 establishes that the RFI must:

- In the case of a proposed business relationship or transaction, not establish that business relationship and not carry out that occasional transaction with or on behalf of the customer;
- In the case of an existing business relationship, terminate that business relationship with the customer; and
- Consider making a report to the FIA, in accordance with its obligations under POCA and the ATFA.

II.130 Where one beneficiary fails to comply with a request for information, while remaining beneficiaries comply, there may be no need to terminate the business relationship. In such a situation, the RFI may consider simply postponing the provision of any service in relation to that uncooperative beneficiary or, as appropriate, the entire insurance business relationship, until all required CDD is carried out.

II.131 Where an RFI declines or terminates business that it knows is, or suspects might be, criminal in intent or origin, the RFI should refrain from referring such declined business to another person.

II.132 Where an RFI request information from a relied upon intermediary, and the request is not met, the RFI will need to take account of that fact in its assessment of the intermediary in question, and of the risks associated with relying upon the intermediary in the future. In addition, the RFI should review its application of CDD in respect of the insurance customer in question.

II.133 Any outsourcing agreement should include a termination and exit management clause that, in the event that an RFI discontinues its outsourcing arrangement with the service provider, allows the outsourced activities and any related data to be transferred to another service provider or to be reincorporated into the outsourcing RFI. Care should be taken to ensure that any termination of an outsourcing arrangement is carried out without detriment to the continuity and quality of the provision of services to clients and compliance with the Regulations and these Guidance Notes.

Receiving and sending insurance payments

II.134 An RFI should establish how any initial, recurring or one-off payment to the insurer, intermediary or third party service provider is to be made, from where and by whom.

II.135 RFIs should accept payments only from an account in the name of the applicant or policyholder.

II.136 Where payment is to be made from an account other than in the name of the applicant or policyholder, the reasons for this must be understood, assessed and recorded. Evidence of identity of the accountholder must be obtained as well as details on the relationship between the applicant or policyholder and the accountholder.

II.137 The RFI should take ongoing measures to satisfy itself that each payment received was actually made from the anticipated account.

II.138 Where funds are being remitted from several accounts, an RFI must understand the reasons for this and be satisfied in each case.

II.139 Where an RFI is sending a payment to an applicant or beneficiary, whether for a claim, premium refund or other reason, the RFI should ensure that payment is sent only to an account in the name of the authorised recipient.

II.140 Where there is a request for payment to be made to more than one account, the reasons for this should be understood and recorded. Evidence of identity of the accountholder(s) must be obtained. Where the accountholder(s) is different from the applicant or beneficiary, details on the relationship between the applicant or beneficiary and the accountholder(s) is also necessary.

II.141 Payments should be made by bank-to-bank transfer wherever possible. Where there is a request for any payment to be made by cheque, the reasons for this should be understood, assessed and recorded. Where an RFI approves the issuance of payment by cheque, the cheque should be marked "account payee only".

II.142 In the context of insurance business, RFIs should limit the acceptance or delivery of cash or other bearer negotiable stores of value to *de minimus* amounts. In extremely rare circumstances where this guidance is not followed, an RFI should be prepared to demonstrate that it has determined and applied appropriate risk-mitigation measures, and documented relevant policies, procedures and controls. Any insurance business cash or bearer instrument transaction that is not of a *de minimus* amount should be reported to the RFI's Reporting Officer.

II.143 Paragraph 7.14 of the main guidance notes states that each RFI should establish norms for cash transactions and procedures for the identification of unusual cash transactions or proposed cash transactions.

II.144 Paragraphs 4.97 through 4.101 (of the main guidance notes) provide additional guidance on the use of bearer instruments.

<u>Applicability of simplified due diligence to insurance business</u>

II.145 Simplified due diligence involves the application of reduced or simplified CDD measures in specified circumstances.

II.146 RFIs may consider applying reduced or simplified due diligence measures only where the risk assessment process results in a finding of lower than standard risk.

II.147 Regulation 10(6), 10(7) and paragraph 1 of Schedule 1 to the Regulations authorise RFIs to apply simplified due diligence measures for insurance customers provided the following criteria are met:

The product is one of the following:

- A life insurance contract where the annual premium is no more than $1,000 or where a single premium of no more than $2,500 is paid for a single policy; or
- An insurance contract for the purpose of a pension scheme where the contract contains no surrender clause and cannot be used as collateral;

and

- The product has a written contractual base;
- Any related transactions are carried out through an account of the customer with an RFI subject to the Regulations, or with an institution that is situated in a country or territory other than Bermuda that imposes requirements equivalent to those in Bermuda, that effectively implements those requirements, and that is supervised for effective compliance with those requirements;
- The product or related transaction is not anonymous and its nature is such that it allows for the timely application of CDD measures where there is a suspicion of money laundering or terrorist financing;
- The benefits of the product and any related transactions cannot be realised for the benefit of third parties, except in the case of death, disablement, survival to a predetermined advanced age, or similar events;
- The benefits of the product and any related transactions are only realisable in the long term;
- The product and any related transactions cannot be used as collateral; and
- During the contractual relationship, no accelerated payments are made, no surrender clauses are used and no early termination takes place.

II.148 In addition, customers for which it may be appropriate to reduce or simplify the application of CDD measures include:

- AML/ATF regulated financial institutions transacting solely on their own behalf (see paragraph 5.147 of the main guidance notes);
- Companies listed on an appointed stock exchange (see paragraphs 4.95 through 4.96 of the main guidance notes);
- Employee pension schemes (see paragraphs 4.136 through 4.141 of the main guidance notes); and
- Bermuda public authorities.

II.149 An RFI must discontinue the application of any reduced or simplified CDD measures and apply either standard or enhanced due diligence measures where:

- A customer makes an accelerated payment or exercises a right to cancel or effectuate an early surrender;
- Any other provision of paragraph II.147 is no longer met; or
- The RFI has reason to doubt that the risks, associated with any business relationship or occasional transaction, are anything other than low.

II.150 Notwithstanding the Regulations' provisions for applying reduced or simplified CDD measures, an RFI may consider it appropriate or necessary to apply standard or enhanced CDD where none is required by the Regulations. An RFI may consider it appropriate or necessary to apply CDD for practical business reasons, for the purpose of screening customers for international sanctions targets, or for any other reason.

II.151 Where reduced or simplified due diligence is appropriate for only one party to an insurance contract, RFIs must nonetheless adhere to the guidance notes in identifying and verifying other parties to the insurance contract.

II.152 Detailed information on the applicability of simplified due diligence is set forth in paragraphs 3.14 and 5.1 through 5.14 of the main guidance notes.

Enhanced due diligence for insurance business

II.153 Enhanced due diligence is the application of additional CDD measures where necessary to ensure that the measures in place are commensurate with higher ML/TF risks.

II.154 Regulation 11 requires RFIs to apply enhanced due diligence in all situations where a customer or the products, services, delivery channels, or geographic connections with which the customer engages present a higher than standard risk of money laundering or terrorist financing.

II.155 In addition, enhanced due diligence must be applied in each of the following circumstances:

- The business relationship or occasional transaction has a connection with a country or territory that represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions (see paragraphs 5.19 through 5.20 of the main guidance notes);
- The customer or beneficial owner has not been physically present for identification purposes (see paragraph 5.26 through 5.30 of the main guidance notes);
- The insurance contract involves the use of one or more bearer instruments (see paragraphs 4.97 through 4.101 of the main guidance notes);

- The insurance contract has been assigned via a viatical arrangement or transferred to an endowment fund (see paragraphs II.184 through II.185)
- The business relationship or occasional transaction involves a PEP (see paragraphs 5.97 through 5.117 of the main guidance notes).

II.156 An insurer must have in place procedures to apply CDD measures in respect of identifying whether any of the following is a PEP:

- An applicant;
- A policyholder;
- A beneficial owner of an applicant or policyholder, or the person funding a premium paid under a policy;
- A settlor or trustee of a trust whose trustee is an applicant or policyholder;
- A beneficiary of a trust whose trustee is an applicant or policyholder;
- A beneficiary named under a policy; or
- Any controller or other person who is able to exercise significant power over the insurance policy.

II.157 Where an RFI determines that enhanced due diligence measures are necessary, it must apply specific and adequate measures to compensate for the higher risk of ML/TF.

II.158 In selecting the appropriate additional measures to be applied, RFIs should consider obtaining additional information and approvals, including one or more of the following:

- Additional information on the customer, such as occupation, volume of assets, and information available through public databases;
- Additional information on the nature and purpose of the business relationship (see paragraphs 4.1 through 4.4 of the main guidance notes);
- Additional information on the source of wealth and source of funds of the customer (see paragraphs 5.110 through 5.113 of the main guidance notes);
- Additional information on the reasons for planned or completed transactions; and
- Approval of senior management to commence or continue the business relationship (see paragraph 5.109 of the main guidance notes).

II.159 In addition, RFIs should consider applying additional measures, such as:

- Refusing cash payments;
- Refusing overpayments of premiums;
- Limiting or precluding premium refund or surrender;

- Updating more frequently the identification and verification data for the applicant, policyholder, beneficial owner of the applicant or policyholder, controller, beneficiary, and any other person who is able to exercise significant power over the insurance policy;
- Conducting enhanced monitoring of the business relationship by increasing the number and frequency of controls applied and by identifying patterns of conduct requiring further examination; and
- Ensuring that payments are carried out through an account in the customer's name through an RFI subject to the Regulations, or through an institution that is situated in a country or territory other than Bermuda that imposes requirements equivalent to those in Bermuda, that effectively implements those requirements, and that is supervised for effective compliance with those requirements.

II.160 Detailed information on enhanced due diligence is set forth in Chapter 5: Non-Standard Customer Due Diligence Measures.

II.161 Specific indicators of higher risk in insurance business are discussed in greater detail in paragraphs II.222 through II.228.

International sanctions

II.162 RFIs conducting insurance business should implement a sanctions compliance programme in line with the guidance set forth in Chapter 6: International Sanctions.

II.163 RFIs should determine whether any persons or activities connected with an insurance arrangement, and the individuals behind any such persons that are legal persons, trusts or other legal arrangements, are sanctions targets.

II.164 RFIs must be aware that, in contrast to AML/ATF measures, which permit firms some flexibility in setting their own timetables for verifying and updating CDD information, an RFI risks breaching a sanctions obligation as soon as a person, entity or good is listed under a sanctions regime in effect in Bermuda. In addition, whereas an RFI may choose to transact with a higher-risk individual or entity, it may not transact with any individual or entity subject to the Bermuda sanctions regime without first applying for and obtaining an appropriate license.

II.165 RFIs should note that the application of reduced or simplified CDD measures, and delays in identifying or verifying the identity of a beneficiary may prevent an RFI from effectively identifying a sanctions target, in turn causing the RFI to breach a sanctions regime in effect in Bermuda.

Ongoing monitoring for insurance business

II.166 Regulations 7, 11(4)(c), 13(4), 16 and 18 require RFIs to conduct ongoing monitoring of the business relationship with their customers.

II.167 Ongoing monitoring in the context of insurance business supports several objectives:

- Maintaining a proper understanding of a customer's activities;
- Ensuring that CDD documents and other records are accurate and up-to-date;
- Providing accurate inputs for the RFI's risk assessment processes;
- Testing the outcomes of the RFI's risk assessment processes; and
- Detecting and scrutinising unusual or suspicious conduct.

II.168 Failure to adequately monitor a customer's business relationship could expose an RFI to abuse by criminals and may call into question the adequacy of the RFI's AML/ATF policies, procedures and controls and the competence and probity of the RFI's management.

II.169 Ongoing monitoring of a business relationship includes:

- Scrutinising transactions undertaken throughout the course of the relationship (including, where necessary, the source of wealth and/or source of funds) to ensure that the transactions are consistent with the RFI's knowledge of the applicant, the policyholder, the beneficial owner of the applicant and/or policyholder, any controllers, the beneficiaries, and the customer profile;
- Investigating the background and purpose of all complex or unusually large transactions, and unusual patterns of transactions which have no apparent economic or lawful purpose and recording in writing the findings of the investigation; and
- Reviewing existing documents, data and information to ensure that they are accurate, up-to-date, adequate, and relevant for the purpose of applying CDD measures to insurance customers and beneficiaries.

II.170 Ongoing monitoring also includes an RFI maintaining up-to-date information on the reliability of any intermediaries the RFI is relying upon for AML/ATF purposes, and taking any needed corrective actions.

II.171 Ongoing monitoring must be carried out on a risk-sensitive basis. Higher-risk insurance customers, beneficiaries and intermediaries must be subjected to enhanced due diligence and more frequent and/or intensive ongoing monitoring.

II.172 Bearing in mind that some criminal activity may be so widespread as to appear to be the norm, RFIs should establish norms for lawful transactions and conduct in relation to insurance customers and beneficiaries. See paragraphs 7.11 through 7.14 of the main guidance notes.

II.173 Once an RFI has established norms for lawful transactions and conduct, it must monitor the business relationship, including transactions, patterns of transactions, and conduct by insurance customers and beneficiaries to identify transactions and conduct falling outside of the norm.

II.174 The determination of norms for a category of customers or beneficiaries should be based initially upon the information obtained in order to understand the purpose and intended nature of the business relationship with the RFI. See paragraph II.65.

II.175 RFIs' and intermediaries' knowledge of their policyholders should be sufficiently detailed to enable them to assess any insurance event properly and should allow them to evaluate the consistency of the event with the customer's profile.

II.176 Where an RFI becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as soon as is reasonably practicable. See paragraph II.122.

II.177 Monitoring may take place both in real time and after the event, and it may be manual or automated. Any system of monitoring should ensure at its core that:

- Transactions and conduct are flagged in exception reports for further examination;
- The exception reports are reviewed promptly by the appropriate person(s); and
- Appropriate and proportionate action is taken to reduce the possibility of ML/TF occurring without detection.

II.178 Where an RFI accepts higher-risk insurance business, it must ensure that it has the capacity and expertise to effectively conduct on-going monitoring of the business relationship with the RFI. See paragraph II.51.

Trigger events

II.179 In insurance business, various transactions or conduct after the contract date may require the application of additional CDD as part of an RFI's ongoing monitoring. These trigger events include, but are not limited to:

- Claims notifications;
- Early surrender requests;
- Overpayment of premiums;
- Changes in the type of insurance product;
- Changes to the duration or amount of coverage;
- Changes in beneficiaries;
- Changes in controllers;
- Changes of address
- Changes of payment method or amount;
- Requests for payments to third parties;
- Subsequently discovered information about an insurance applicant, beneficial owner of an applicant, controller or beneficiary; and
- Information received from a competent authority.

II.180 Where an RFI is monitoring the reliability of an intermediary upon which it relies for AML/ATF purposes, additional trigger events include, but are not limited to:

- Changes in the volume of business through the intermediary;
- Changes in fee amounts the intermediary charges customers; and
- Changes to the AML/ATF regulatory status of the intermediary or of the country or territory in which the intermediary is regulated.

II.181 The background and purpose of each trigger event should, as far as possible, be examined in order to determine whether the risk ratings assigned to the business relationship require modification and whether any additional risk-mitigation measures need to be put in place. The findings of the examination should be recorded and maintained in accordance with the record-keeping obligations set forth in Chapter 11: Record-Keeping and paragraphs II.216 through II.221.

Policy cancellations and early surrender requests

II.182 Where an applicant exercises the right to decline to proceed with a contract during a cooling off or cancellation period, or to exercise an early surrender of the policy, the circumstances should be examined.

II.183 Where a payment is made to an applicant due to the exercise of a cancellation or early surrender right, the payment should be made to the ceding account from which the funds were originally sent. See paragraphs II.134 through II.144.

Assignments and transfers of benefits

II.184 Where the benefits of a policy are assigned to a third party via a viatical, endowment, or other arrangement, verification of the assignee's identity must be obtained either before assignment takes place, or as soon as is reasonably practicable thereafter.

II.185 Whether an assignment has been notified or not, when a payment is to be made from the policy to an account not in the name of a verified person or entity, the RFI must ensure that full verification of identity of the accountholder has been completed in accordance with the Regulations and these guidance notes before payment is made.

II.186 RFIs should exercise caution with regard to any insurance contract that involves the use of bearer instruments, or which itself serves as a bearer instrument. Because bearer instruments can be exchanged easily from person to person without notifying the RFI of the resulting changes in rights, bearer instruments limit an RFI's ability to conduct CDD that meets the requirements of the Acts, Regulations and these guidance notes.

II.187 Paragraphs 4.97 through to 4.101 of the main guidance notes set forth additional guidance concerning bearer instruments.

Sufficiency of source of wealth information for subsequent business transactions

II.188 The source of wealth of an existing policyholder who wishes to undertake an additional or subsequent transaction, for example, an accelerated payment, or new single premium policy, must be examined to consider whether the information held at that time is sufficient to indicate that the additional transaction would be reasonable. Where an RFI considers that additional information is required, it must obtain that information as soon as is reasonably practicable.

II.189 Paragraphs 5.110 through 5.113 of the main guidance notes and II.66 through II.69 set forth additional guidance on sources of wealth and funds.

II.190 Detailed information on ongoing monitoring is set forth in Chapter 7: Ongoing Monitoring.

Suspicious activity reporting

II.191 The suspicious activity reporting requirements for RFIs are governed primarily by Sections 43 through 48 of POCA 1997, Paragraphs 1 and 2 of Schedule 1of ATFA 2004, and Regulations 16 and 17.

II.192 RFIs conducting insurance business must put in place appropriate policies and procedures to ensure that knowledge, suspicion, and reasonable grounds to know or suspect that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing, are identified, enquired into, documented, and reported.

II.193 The definitions of knowledge, suspicion, and reasonable grounds to know or suspect are set forth in paragraphs 9.6 through 9.10 of the main guidance notes.

II.194 Many customers may, for perfectly good reasons, have an erratic pattern of transactions or account activity. A transaction or activity that is identified as unusual, therefore, should not be automatically considered suspicious, but should cause the RFI to conduct further, objective enquiries to determine whether or not the transaction or conduct is indeed suspicious.

II.195 Enquiries into unusual transactions should be in the form of additional CDD measures to ensure an adequate, gap-free understanding of the relationship, including the purpose and nature of the transaction and/or conduct in question.

II.196 All employees, regardless of whether they have a compliance function, are obliged to report to the Reporting Officer within the RFI each instance in which they have knowledge, suspicion, or reasonable grounds to know or suspect that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing.

II.197 An RFI's Reporting Officer must consider each report, in light of all available information, and determine whether it gives rise to knowledge, suspicion, or reasonable grounds to know or suspect that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing.

II.198 Where, after evaluating an internal suspicious activity report, the Reporting Officer determines that there is knowledge, suspicion, or reasonable grounds to know or suspect that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing, the Reporting Officer must file an external suspicious activity report with the FIA.

II.199 As of October 2011, the FIA no longer accepts any manually submitted suspicious activity reports (including those faxed or e-mailed). The FIA accepts only those suspicious activity reports that are submitted electronically via the goAML system, which is available at www.fia.bm.

II.200 Where a Reporting Officer considers that an external report should be made urgently, initial notification to the FIA may be made by telephone, but must be followed up by a full suspicious activity report as soon as is reasonably practicable.

II.201 The FIA is located at 6th Floor, Strata 'G' Building, 30A Church Street, Hamilton HM11 and it can be contacted during office hours on telephone number (441)-292-3422, on fax number (441)-296-3422, or by e-mail at info@fia.bm

II.202 RFIs should ensure that any intermediaries being relied upon have appropriate policies, procedures and controls to identify, enquire into, document, and report knowledge, suspicion, or reasonable grounds to know or suspect that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing.

Failure to report and tipping-off offences

II.203 Where an employee fails to comply with the obligations under Section 46 of POCA 1997 or Schedule 1 of ATFA 2004 to make disclosures to a Reporting Officer as soon as is reasonably practicable after information giving rise to knowledge or suspicion comes to the attention of the employee, the employee is liable to criminal prosecution.

II.204 The criminal sanction, under POCA 1997 and ATFA 2004, for failure to report, is a prison term of up to three years on summary conviction or ten years on conviction in indictment, a fine up to an unlimited amount, or both.

II.205 Section 47 of POCA 1997 and Section 10 of ATFA 2004 contain tipping-off offences.

II.206 It is a tipping-off offence under Section 47 of POCA 1997 and Section 10 of ATFA 2004 if a person knows or suspects that an internal or external report has been made to the Reporting Officer or to the FIA and the person discloses to any other person:

- Knowledge or suspicion that a report has been made; and/or
- Any information or other matter likely to prejudice any investigation that might be conducted following such a disclosure.

II.207 It is also a tipping-off offence if a person knows or suspects that a police officer is acting, or proposing to act, in connection with an actual or proposed investigation of money laundering or terrorist financing and the person discloses to any other person any information or other matter likely to prejudice the actual or proposed investigation.

II.208 Any approach to the customer or to an intermediary should be made with due regard to the risk of committing a tipping-off offence. See paragraphs 9.83 through 9.84 of the main guidance notes.

II.209 RFIs and intermediaries should also have due regard to paragraphs 9.85 through 9.86 of the main guidance notes.

II.210 Detailed information on suspicious activity reporting is set forth in Chapter 9: Suspicious Activity Reporting.

Employee training and awareness

II.211 The responsibilities of RFIs to ensure appropriate employee training and awareness are governed primarily by Regulations 16 and 18.

II.212 RFIs must take appropriate measures to ensure that relevant employees, including employees of relied upon intermediaries:

- Are aware of the Acts and Regulations relating to ML/TF;
- Undergo training on how to identify transactions which may be related to ML/TF; and
- Know how to properly report suspicions regarding transactions that may be related to ML/TF.

II.213 Each RFI must also ensure that relevant employees, including employees of relied upon intermediaries receive appropriate training on its AML/ATF policies and procedures relating to:

- Customer due diligence measures;
- Ongoing monitoring;
- Record-keeping;
- Internal controls; and
- Risk assessment and management.

II.214 In an insurance business context, training should enable relevant employees to:

- Readily identify insurance products and intermediaries that may be abused for ML/TF purposes;
- Effectively vet insurance customers and beneficiaries;

- Assess the risks associated with an insurance policy and payments made from and received into it; and
- Conduct ongoing monitoring of the insurance business relationship with the RFI.

II.215 Detailed information on employee training and awareness is set forth in Chapter 10: Employee Training and Awareness.

Record-keeping

II.216 The record-keeping obligations of RFIs are governed primarily by Regulations 15 and 16.

II.217 RFIs must keep specified records for a period of at least five years following the date on which the business relationship ends, or, in the case of an occasional transaction, following the date on which the transaction, or the last in a series of transactions, is completed.

II.218 RFIs conducting insurance business should ensure that adequate procedures are in place to allow the RFI, in combination with any introducers to access:

- Initial documentation including, but not limited to, the customer financial assessment, customer needs analysis, copies of regulatory documentation, illustration of benefits, and copies of documentation supporting verification;
- All post-sale records associated with the contract, up to and including the maturity of the contract;
- Details of the maturity processing and/or claim settlement including completed discharge documentation;
- Payment transaction details sufficient to identify and, where applicable, verify the proposed and actual sources and recipients of funds.

II.219 Where records are maintained by intermediaries or third party service providers, RFIs should ensure that any records are stored securely and are capable of being retrieved upon request and without delay.

II.220 RFIs must not rely upon any person to maintain records where access to records without delay is likely to be impeded by confidentiality, secrecy, privacy or data protection restrictions.

II.221 Detailed information on the records that must be kept is set forth in Chapter 11: Record-Keeping.

Risk factors for insurance business

II.222 In addition to the non-exhaustive list of risk factors set forth in paragraphs 2.35 and II.55, RFIs conducting insurance business should consider sector-specific risk factors, including those in paragraphs II.223 through II.228 below, in order to fully assess the ML/TF risks associated with a particular insurance business relationship. The non-exhaustive list of sector-specific risk factors addresses customers, products, services, transactions, delivery channels, third party service providers and geographic connections.

II.223 Customer risk factors include, but are not limited to:

- The lack of readily apparent connection or relationship between the applicant or policyholder and the beneficiaries. The economic nature of a life insurance policy is a mechanism for the policyholder to benefit a beneficiary. RFIs should ascertain policyholder's reasons for wanting to benefit a beneficiary with whom he or she seemingly has no connection;
- Frequent and unexplained changes to the beneficiaries;
- Attempts to remove all existing beneficiaries and add new beneficiaries. Although this may be a legitimate action, the RFI should ensure that any reasons given for such changes are reasonable;
- Requests to add a third party as a new beneficiary, particularly where the RFI receives the nomination after the death of the policyholder;
- Situations in which it is difficult to identify the individual beneficiaries of a life insurance contract. This includes situations where identification is hindered because a beneficiary is a legal person, trust or another type of legal arrangement;
- Any unexplained relationship between an applicant or policyholder and the controllers;
- Unjustified delays in the production of identity documents or other requested information;
- A customer who is unwilling or unable to provide satisfactory information to verify the source of wealth or source of funds;
- The involvement of a PEP in the business relationship;
- The unexplained and illogical use of corporate structures, express trusts, nominee shares or the use of bearer negotiable instruments;
- Any change in the nature or amount of insurance coverage that is inconsistent with a customer's needs and sources of wealth and funds as recorded in the customer's profile;
- Levels of assets, coverage or transactions that exceed what a reasonable person would expect of a customer with a similar profile;

- Sudden and unexplained deposits, withdrawals, contractual changes or lifestyles changes;
- Significant or repeated overpayments of policy premiums after which the policyholder requests reimbursement to him- or herself or to a third party;
- Lack of concern by the applicant or policyholder over charges or costs for early surrender;
- Undue interest by the applicant or policyholder in early payout options;
- A policyholder seeks to borrow the maximum cash value of a single premium policy, soon after paying for the policy;
- The unexplained use of a power of attorney or other third party mandate;
- Apparent collusion between a customer and an intermediary or insurance company employee;
- Requests for multiple policies to be taken out for premiums slightly below the limits set forth in paragraph II.147.
- A customer accepting highly unfavourable terms unrelated to his or her health or age;
- A customer offering to pay extraordinary fees for unusual services, or for services that would not ordinarily warrant such a premium; and
- Requests for no correspondence to go to the policyholder.

II.224 Products and services risk factors include, but are not limited to:

- Investment-linked insurance policies;
- Single premium life insurance policies that store value;
- Insurance policies that permit one or more acceleration payments or lump sum top-offs;
- Insurance products that can be used as collateral;
- Insurance policies that contain an early surrender clause;
- Insurance policies that allow a transfer of benefits without the knowledge of the RFI until such time that a claim is made; and
- Insurance policies that have been transferred to an endowment fund or via a viatical arrangement;

II.225 Transaction risk factors include, but are not limited to:

- An insurance business relationship that, once established, receives cash payments, or payments from multiple sources;
- Cash or bearer instrument transactions in circumstances where such a transaction would normally be made by cheque, banker's draft, or wire transfer;
- The use of an insurance policy as a bearer asset;

- A lump sum top-up to an existing life insurance or annuity contract;
- Overpayment of a premium, particularly when followed by a request for a refund;
- Early or frequent claims under a general insurance policy, particularly where the claims amounts are below the premium amount;
- Payment by a means which allows for anonymity of the transaction;
- Payment of a premium in one currency, followed by a request for repayment in a different currency;
- Requests for payments to accounts that are not in the name of the policyholder or beneficiary;
- Payments received from an account that is not in the name of the applicant or policyholder;
- Requests for prepayment of benefits;
- Requests for early surrender, including the exercise of any right under a cooling off or cancelation provision that would result in a payment being made to the customer, particularly where such requests result in economic penalty to the customer.
- The unusual use of an insurance policy as collateral;
- Insurance customers requesting payments to or from overseas locations with instructions for payment to be made in cash;
- Insurance customers requesting payments to or from third parties seemingly unconnected with the insurance business relationship;
- Assignments of insurance benefits via a viatical arrangement;
- Transfers of insurance benefits to an endowment fund;
- Transactions within an insurance business relationship that have no apparent legitimate business, tax or legal purpose;
- Transactions of a size or volume that exceeds what a reasonable person would expect of a customer with a similar profile, or given the nature and stated purpose of the insurance business relationship; and
- Transactions that the RFI cannot fully explain and document.

II.226 Delivery channel risk factors include, but are not limited to:

- Non face-to-face relationships with insurance customers;
- Any request to carry out significant transactions using cash, or using any payment or value transfer method such as a bearer instrument that obscures the identity of any of the parties to the transaction;
- The involvement of intermediaries or third party service providers that do not apply AML/ATF measures at least equivalent to those in Bermuda;
- Apparent collusion between a customer and any director, manager or employee of an intermediary, insurance company or reinsurance company;

- An intermediary accepting extraordinary fees for unusual services, or for services that would not ordinarily warrant such a premium; and
- A sudden change in the volume of business connected with an intermediary.

II.227 Third party risk factors include, but are not limited to:

- The involvement of any person in carrying out any AML/ATF function in relation to insurance business, including reliance upon, or outsourcing to, any person that has not been sufficiently reviewed for compliance with paragraphs 5.118 through 5.178 of the main guidance notes;
- Any unexplained relationship between an applicant or policyholder and any controller, beneficiary or other third party;
- Requests to add a third party as a new beneficiary, particularly where the RFI receives the nomination after the death of the policyholder; and
- The involvement of a recently established intermediary, insurance company or reinsurance company, particularly where the background of the entity does not appear to be particularly transparent.

II.228 Geographic risk factors include, but are not limited to:

- An insurance business relationship established with funds originating from foreign banks in high-risk jurisdictions;
- An applicant, policyholder, beneficial owner of an applicant or policyholder, controller, beneficiary, intermediary or any other person connected with the business relationship who is a resident in, or citizen of, a high-risk jurisdiction;
- An insurance business transaction to or from a high-risk jurisdiction;
- An insurance business transaction linked to business in or through a high-risk jurisdiction;
- Insurance business involving persons or transactions with a material connection to jurisdiction, entity, person, or activity that is a target of an applicable international sanction; and
- An insurance business relationship or transaction for which an RFI's ability to conduct full CDD may be impeded by a jurisdiction's confidentiality, secrecy, privacy, or data protection restrictions.