Model Guidelines for Life Insurance Enterprises' Anti-Money Laundering and Countering Terrorism Financing Policies and Procedures

FSC approval document no. Jin-Guan-Bao-Zong-10610958830 issued on 13 Nov 2017 for recordation.

Article 1

The Model Guidelines is established in accordance with the "Money Laundering Control Act", the "Terrorism Financing Prevention Act", the "Regulations Governing Anti-Money Laundering of Financial Institutions", and the "Directions Governing Internal Control System of Anti-Money Laundering and Countering the Financing of Terrorism of Insurance Sector".

Article 2

An insurance company's internal control system for anti-money laundering and countering the financing of terrorism (AML/CFT) established in accordance with Article 5 of the "Regulations Governing Implementation of Internal Control and Auditing System of Insurance Sector" and any subsequent amendment thereto should be approved by its board of directors(council). The internal control system should contain the following particulars:

1. The policies and procedures to identify, assess and manage its money laundering and terrorist financing risks in accordance with the "Guidelines for Insurance Companies Regarding Assessment of Money Laundering and Terrorism Financing Risks and Adoption of Prevention Programs (Guidelines)". (See Attachment).
2. An AML/CFT program established based on the Guidelines and an insurance company's money laundering and terrorist financing risk assessment result and business size to manage and mitigate the risks identified and take enhanced control measures for higher risk categories.
3. Standard operational procedures for monitoring compliance with AML/CFT regulations and for the implementation of AML/CFT program, which should be included in the self-inspection and the internal audit, and enhanced if necessary.

The identification, assessment and management of money laundering and terrorist financing risks provided in Subparagraph 1 of the preceding paragraph should cover at least customers, geographic areas, products and services, transactions, and delivery channels, and be conducted in accordance with the following requirements:

1. Producing a risk assessment report.
2. Considering all risk factors to determine the level of overall risk and appropriate measures to mitigate risks.
3. Having a mechanism in place for updating risk assessment report to ensure that risk data are kept up-to-date.
4. Filing the risk assessment report with the Financial Supervisory Commission ("FSC") for recordation after it is completed or updated.

The AML/CFT program provided in Subparagraph 2 of Paragraph 1 hereof should include the following policies, procedures and controls:

1. Customer Due Diligence ("CDD").
2. Name screening on customers and related parties of a transaction.

3. Ongoing monitoring of transactions.
4. Record keeping.
5. Reporting of cash transactions above a certain amount.
6. Reporting of transactions suspicious of money laundering or terrorist financing (STR) and reporting in accordance with the Terrorism Financing Prevention Act.
7. Appointment of a dedicated AML/CFT officer to take charge of AML/CFT compliance matters.
8. Employee screening and hiring procedure.
9. Ongoing employee training program.
10. An independent audit function to test the effectiveness of AML/CFT system.
11. Other matters required by the AML/CFT regulations and the FSC.

An insurance company having foreign branches (or subsidiaries) should establish a group-level AML/CFT program for implementation by branches (or subsidiaries) within the group. The AML/CFT program should include the policies, procedures and controls provided in the preceding paragraph, and in addition, the following particulars without violating the information confidentiality regulations of the R.O.C. and host countries or jurisdictions of the foreign branches (or subsidiaries):

1. Policies and procedures for sharing information within the group required for the purposes of CDD and money laundering and terrorist financing risk management.
2. Group-level compliance, audit, and AML/CFT functions should be provided with customer and transaction information from foreign branches (or subsidiaries) when necessary for AML/CFT purposes.
3. Adequate safeguards on the confidentiality and use of information exchanged.

An insurance company should ensure that its foreign branches (or subsidiaries) apply AML/CFT measures to the extent that the laws and regulations of host countries or jurisdictions permit, and those measures should be consistent with those adopted by the head office (or parent company). Where the minimum requirements of the countries where its head office (or parent company) and branches (or subsidiaries) are located are different, the branch (or subsidiary) should choose to follow the criteria whichever are higher. However, in case there is any doubt regarding the determination of higher or lower criteria, the determination by the competent authority of the place at where the head office of the insurance company is located should prevail. If a foreign branch (or subsidiary) is unable to adopt the same criteria as the head office (or parent company) due to prohibitions from foreign laws and regulations, additional appropriate measures should be taken to manage the money laundering and terrorist financing risks, and a report should be made to the FSC.

With respect to the requirements provided in Subparagraph 1 and 2 of Paragraph 1, a branch or subsidiary of a foreign financial group in Taiwan, should establish policies and procedures for identifying, assessing and managing money laundering and terrorist financing risks in accordance with the Guidelines, and establish policies, procedures, and controls that AML/CFT programs should include. If the group has established ones that are not less strict than and do not conflict with domestic regulatory requirements, such branch or subsidiary may apply the group's requirements.

The board of directors (council) of an insurance company holds the ultimate responsibility of ensuring the establishment and maintenance of appropriate and effective AML/CFT internal controls. The board of directors (council) and the senior management should understand the company's money laundering and terrorist financing risks and the operation of its AML/CFT program, and adopt measures to create a culture of AML/CFT compliance.

Article 3

Terms used in the Model Guidelines are defined as follows:

1. "A certain amount" refers to NTD 500,000 (or equivalent foreign currency).
2. "Cash transaction" refers to receiving cash or paying cash in a single transaction (including all transactions recorded on a cash deposit or withdrawal slip for accounting purpose).
3. "Establishing business relationship" refers to a person that requests an insurance company to provide insurance or financial services and establish relationship that can continue for a duration, or a person that first approaches an insurance company as a potential customer and expects such a relationship may continue for a duration.
4. "Customer" refers to a person that establishes business relationship with an insurance company, including a natural person, a legal person, an entity other than a legal person, or a trust).
5. "Beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer, or the natural person on whose behalf a transaction is being conducted. It includes the natural persons who exercise ultimate effective control over a legal person or arrangement.
6. "Risk-based approach" (RBA) refers to the fact that an insurance company should identify, assess and understand the money laundering and terrorist financing risks that it is exposed to and take appropriate AML/CFT measures to effectively mitigate such risks. With such approach, an insurance company should take enhanced measures for higher risks while simplified measures may be taken for lower risks to effectively allocate resources and mitigate the identified money laundering and terrorist financing risks in the most appropriate and effective way.
7. "Related parties of a transaction" refer to any third party other than an insurance company's customers, who is involved in a transaction.

Article 4

An insurance company should conduct CDD measures in accordance with the following requirements:

1. If there exists any of the following situations, an insurance company should decline to establish business relationship or carry out any transaction with the customer
   (1) The customer is suspected of using an anonymity, a fake name, a nominee, a shell firm, or a shell corporation or entity.
   (2) The customer refuses to provide relevant documentations required for the purpose of CDD except that an insurance company may verify the customer's identify by using reliable, independent source of information.
   (3) In the case that any person acts on behalf of a customer, it is difficult to verify that the person purporting to act on behalf of the customer is so authorized and the identity of that person.
   (4) The customer uses counterfeit or altered identification documents.
   (5) Identification documents presented are all photocopies except for the business that permits the use of photocopies or image files of identification documents with other alternative measures under applicable regulations.
   (6) Documents provided by the customer are suspicious or unclear, or the customer refuses to provide other supporting documents, or the documents provided cannot be authenticated
   (7) The customer procrastinates in providing identification documents in an unusual manner.

(8) The party with whom an insurance company establishes business relationship is an individual, a legal person or an organization sanctioned under the Terrorism Financing Prevention Act, or is a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization, except for payments made under Subparagraphs 2～4, Paragraph 1, Article 6 of the Terrorism Financing Prevention Act.

(9) Other unusual circumstances exist in the process of establishing business relationship or conducting transaction and the customer fails to provide reasonable explanations.

2. An insurance company should undertake CDD measures when:

(1) Establishing business relationships with a customer.

(2) Making cash receipt or payment in a single transaction (including all transactions recorded on a cash deposit or withdrawal slip for accounting purpose) of NTD500,000 or more (including the foreign currency equivalent thereof).

(3) There is a suspicion of money laundering or terrorist financing.

(4) There are doubts about the veracity or adequacy of previously obtained customer identification data.

3. An insurance company should take CDD measures as follows：

(1) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information, and should keep copies of the customer's identification documents or record the relevant information thereon.

(2) In the case that any person acts on behalf of a customer to apply for insurance coverage, claims request, policy changes, or other transactions, an insurance company should verify that the person purporting to act on behalf of the customer is so authorized. In addition, identify and verify the identity of that person in accordance with preceding Item, and retain photocopies of the agent's identity documents or record the relevant information thereon.

(3) Identifying the beneficial owner of the customer, and taking reasonable measures to verify the identity of the beneficial owner, including using reliable source data or information.

(4) CDD measures should include understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

4. For an individual customer, an insurance company should at least obtain the following information to identify the customer identity when applying the requirements under preceding subparagraph:

(1) Full name.

(2) Date of birth.

(3) Permanent or residential address.

(4) Official identification document number.

(5) Nationality.

(6) The purpose of residence or transaction of a foreign person (such as tourism, work, etc.)

5. For an individual customer that is identified by an insurance company as a high-risk customer in accordance with the insurance company's relevant requirements on customer money laundering and terrorist financing risk assessment, the insurance company should obtain at least any of the following information when establishing business relationships:

(1) Any other names used or alias: such as the name used before marriage or change of name.

(2) Office address, PO Box address, e-mail address, if any.

(3) Telephone or mobile phone number.

6. For a customer that is a legal person, an organization or a trustee, an insurance company, when applying the requirements under Subparagraph 3, should understand the business nature and obtain at least the following information of the customer or the trust (including any legal arrangement similar to a trust) to identify and verify the customer identity:

(1) Name, legal form and proof of existence of the customer or trust.

(2) The charter or similar power documents that regulate and bind the legal person, the organization or the trust, except for any of the following circumstances:

i. Customers/entities listed under Item 3 of Subparagraph 7 hereof and insurance products listed under Item 4 of Subparagraph 7 hereof are free of the situation provided in the proviso of Subparagraph 3, Paragraph 1 of Article 6 herein.

ii. The customer who is an organization acknowledges that it does not have a charter or similar power document.

(3) The following information of the relevant persons having a senior management position in a legal person, an organization or a trustee (the scope of senior management may cover members of the board, supervisors, members of the council, Chief Executive Officer, Chief Financial Officer, representatives, managers, partners, authorized signatories, or any natural person having equivalent aforementioned positions determined by an insurance company by using risk-based approach):

i. Full name.

ii. Date of birth.

iii. Nationality.

(4) Official identification number: such as business identification number, tax identification number, registration number.

(5) The address of the registered office of a legal person, an organization or a trustee, and if different, the address of its principal place of business.

(6) The purpose of the business relationship of an offshore legal person, an organization or a trustee.

7. When the customer is a legal person, an organization or a trustee, an insurance company should, in accordance with Item 3 of Subparagraph 3 hereof, understand the ownership and control structure of the customer or the trust, and obtain the following information to identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons should:

(1) For legal persons and organizations:

i. The identity of the natural person(s) who ultimately has a controlling ownership interest in the legal person, such as full name, date of birth, nationality, identification number, etc. A controlling ownership interest refers to owning directly and/or indirectly more than 25 percent of the legal person’s shares or capital ; an insurance company may ask the customer to provide its list of shareholders or other documents to assist in the identification of persons holding controlling ownership interest.

ii. To the extent where no natural person exerting control through ownership interests is identified or that there is doubt as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) in accordance with the preceding Sub-item, the identity of the natural person(s), if any, exercising control of the customer through other means. If necessary, an insurance company may obtain a certification from the customer to identify the beneficial owner(s).

iii. Where no natural person is identified under the preceding two Sub-items, an insurance company should identify and verify the identity of the natural person of the senior management.

(2) For a customer that is a trustee of a trust: an insurance company should verify identity of the settlor(s), the trustee(s), the trust supervisor, the beneficiaries, and any other natural person(s) exercising ultimate effective control over the trust, or the identity of person(s) in equivalent or similar position.

(3) Unless otherwise provided in the proviso of Item 3, Subparagraph 1 of Article 6 herein or where the customer has issued bearer shares, an insurance company is not subject to the requirements of identifying and verifying the identity of beneficial owner(s) of a customer set out under Item 3 of Subparagraph 3 hereof, provided the customer or the person having a controlling ownership interest in the customer is:

i. an R.O.C. government entity.

ii. an enterprise owned by the R.O.C. government.

iii. a foreign government entity.

iv. a public company and its subsidiaries.

v. an entity listed on a stock exchange outside of R.O.C. that is subject to regulatory disclosure requirements of its principal shareholders, and the subsidiaries of such entity.

vi. a financial institution supervised by the R.O.C. government, and an investment vehicle managed by such institution.

vii. a financial institution incorporated or established outside of R.O.C. that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the Financial Action Task Force (FATF), and an investment vehicle managed by such institution. An insurance company should keep relevant documents and proof of the aforementioned financial institutions and investment vehicles (such as record of public information search, AML policies and procedures of the financial institution, record of negative news search, certification of the financial institution, etc.)

viii. a fund administered by a R.O.C. government entity.

ix. an employee stock ownership trust or an employee savings trust.

(4) An insurance company is not subject to the requirements of identifying and verifying the identity of beneficial owner(s) of a customer set out under Item 3 of Subparagraph 3 hereof when the customer purchases accidental insurance, health insurance or an insurance product that has no cash value, unless the customer is from or in a high risk country or territory known to have inadequate AML/CFT regime or where there is a suspicion of money laundering or terrorist financing in relation to the customer or the transaction.

8. An insurance company should, unless otherwise provided by laws or regulations, identify the customer and verify that customer’s identity using reliable, independent source documents, data

or information. An insurance company should adopt one of the following measures in verifying the identity of a customer, any person purporting to act on behalf of the customer and the beneficial owner, and should keep photocopies of the identification documents or record the relevant information thereon:

(1) Verifying by documentary method:

i. An individual:

(i) Verification of identity or date of birth: obtain an unexpired official identification document that bears a photograph of the individual (e.g. identification card, passport, residence card, driving license, etc.) If there is doubt as to the validity of such documents, an insurance company should obtain certification provided by an embassy official or a public notary. With respect to the identity or date of birth of the beneficial owners of an entity, an insurance company are not required to obtain original copies of the aforementioned document for verification, and may, according to the insurance company's internal operating procedures, request the entity and its authorized representative to provide a certification that specifies the identification data of the beneficiary owners. Part of the data on such certification, however, should allow an insurance company to perform verification through the certificate of incorporation, annual report, or other reliable source documents or data.

(ii) Verification of address: obtain bills, account statements, or official documents, etc. from the individual.

ii. A legal person, an organization or a trustee:

An insurance company, for the purpose of verification, should obtain Certified Articles of Incorporation, government-issued business license, Partnership Agreement, Trust Instrument, Certification of Incumbency, etc. If a trust is managed by a financial institution described in Paragraph 1 of Article 5 of Money Laundering Control Act, a certification issued by the financial institution may substitute for the trust instrument of the trust unless the country or territory where the financial institution is located is a high-risk country or territory known to have inadequate AML/CFT regime or where there is a suspicion of money laundering or terrorist financing in relation to the customer or the transaction.

(2) Verifying by non-documentary method, such as:

i. Contacting the customer by phone or mail after the business relationship is established.

ii. Information provided by other financial institution(s).

iii. Cross-checking information provided by the customer with other reliable public information or private database, etc.

9. For a customer identified by an insurance company as a high-risk customer in accordance with the insurance company's money laundering and terrorist financing risk assessment, the insurance company should perform one of the following enhanced verification measures:

(1) Obtaining a reply, signed by the customer or the authorized signatory of the entity, for a letter mailed to the address provided by the customer, or contacting the customer by telephone.

(2) Obtaining evidence that supports an individual's sources of wealth and sources of funds.

(3) On-site visits.

(4) Obtaining past insurance transaction information.

10. An insurance company should not establish business relationship with a customer before completing the CDD measures. However, an insurance company may first obtain information on the identity of the customer and its beneficial owner(s) and complete the verification after the establishment of business relationship, provided that:

    (1) money laundering and terrorist financing risks are effectively managed, including adopting risk management procedures with respect to the situations under which a customer may utilize the business relationship to complete a transaction prior to verification.

    (2) it would be essential not to interrupt the normal operation of business with the customer.

    (3) verification of the identities of the customer and its beneficial owner(s) will be completed as soon as reasonably practicable after the establishment of business relationship. An insurance company should advise its customer in advance that the business relationship will be terminated if verification cannot be completed as soon as reasonably practicable.

11. If an insurance company permits the establishment of the business relationship with a customer before completing customer identity verification, the insurance company should adopt relevant risk control measures, including:

    (1) Establishing a timeframe for the completion of customer identity verification.

    (2) Before the completion of customer identity verification, business unit supervisory officer should periodically review the business relationship with the customer and periodically keep senior management informed of the progress of customer identity verification.

    (3) Limiting the number of transactions and types of transaction before the completion of customer identity verification.

    (4) Prohibit the customer from making payment to any third party unless following requirements are met:

        i. There is no suspicion of money laundering and terrorist financing.

        ii. The customer is assessed as a low money laundering and terrorist financing risk customer.

        iii. The transaction is approved by senior management, whose level is determined on the basis of the insurance company's internal consideration for risk.

        iv. The names of payee do not match with lists established for AML/CFT purposes.

    (5) If there is any doubt as to the authenticity, appropriateness or intention of the customer or beneficial owner, the exception provided in proviso of the preceding item does not apply.

    (6) An insurance company should determine the "reasonably practicable timeframe" provided in Item 3 of the preceding subparagraph based on a risk-based approach to the extent that timeframes are differentiated according to risk level. Examples are as follows:

        i. An insurance company should complete customer identity verification no later than 30 working days after the establishment of business relationship.

        ii. If customer identity verification remains uncompleted 30 days after the establishment of business relationship, an insurance company should suspend business relationship with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the extent that this is possible).

        iii. If customer identity verification remains uncompleted 120 days, an insurance company should terminate business relationship with the customer.

12. For a customer that is a legal person, an insurance company should understand whether the customer is able to issue bearer shares by reviewing the article of incorporation or requesting a certification from the customer, and take one of the following measures to ensure the update of beneficial owners:

    (1) Requesting the customer to require bearer share holders who ultimately have a controlling ownership interest to notify the customer to record their identity, and requesting the customer to notify the insurance company immediately when the identity of such share holder changes.

    (2) Requesting the customer, after each shareholders' meeting, to update the information of beneficial owners and provide identification data of any shareholder that holds a certain percentage (or above) of bearer shares. The customer should notify the insurance company immediately if, through other means, it is aware of the identity of any shareholder who ultimately has a controlling ownership interest changes.

13. When conducting CDD measures, an insurance company should use self-established database or information obtained from external sources to determine whether a customer and its beneficial owner or senior managerial officer is a person who is or has been entrusted with a prominent function by a domestic or foreign government or an international organization（referred to as politically exposed persons (PEPs) hereunder）:

    (1) For a customer or the beneficial owner determined to be a current PEP of a foreign government, an insurance company should treat the customer directly as a high-risk customer, and adopt Enhanced Due Diligence measures under Subparagraph 1, Paragraph 1 of Article 6 herein.

    (2) For a customer or the beneficial owner determined to be a current PEP of R.O.C. government or an international organization, an insurance company should assess the PEP's risks when establishing business relationship with the person and conduct annual review thereafter. In case of higher risk business relationship with such customers, an insurance company should adopt Enhanced Due Diligence under Subparagraph 1, Paragraph 1 of Article 6 herein.

    (3) For a senior managerial officer of a customer determined to be a current PEP of a R.O.C. government, a foreign government or an international organization, an insurance company should determine whether to apply Enhanced Due Diligence measures under Subparagraph 1, Paragraph 1 of Article 6 herein by considering the level of influence the officer has on the customer.

    (4) For a PEP who is no longer entrusted with a prominent public function by R.O.C. government, a foreign government or an international organization, an insurance company should assess the level of influence that the individual could still exercise by considering relevant risk factors and determine whether to apply the requirements of the preceding three Items based on the RBA.

    (5) The preceding four items apply to family members and close associates of PEPs. The scope of family members and close associates mentioned above will be determined in a manner stipulated in the latter section of Paragraph 4, Article 7 of the Money Laundering Control Act.

    (6) Requirements of Item 1 to 5 herein do not apply when the beneficial owner or senior managerial officer of a customer specified under Sub-item 1 to 3 and 8, and Item 3 of Subparagraph 7 herein is a PEP.

    (7) Insurance companies and post offices engaging in simple life insurance business should take reasonable measures to identify and verify whether the beneficiary of a life insurance policy, investment-linked insurance policy or annuity insurance policy and the beneficial owner of the beneficiary are PEPs referred to in the preceding paragraph before paying out insurance proceeds or cash surrender value. In case high risk circumstances are discovered, an insurance

company should, prior to paying out insurance proceeds, inform the senior management, conduct enhanced scrutiny on the whole business relationship with the customer, and consider filing a report on transactions suspicious of money laundering or terrorist financing (STR).

14. Other Directions for Customer Due Diligence Process

(1) Directions for Underwriting Process:

i. When an individual is applying for insurance, a solicitor should request the applicant or the insured to provide identification documents (identification card, passport, driver's license, or other supporting documents that can prove his identity) or record the relevant information thereon; an insurance company should also make an inquiry to relevant domestic or foreign organizations or use self-established database to determine whether the customer is a PEP. If the customer is a PEP, adequate management measures and regular reviews should be implemented. The records or vouchers on transactions should be kept if the assessment result shows any suspicious signs of money laundering or terrorist financing, and file a STR to the Investigation Bureau, Ministry of Justice. When a legal person is applying for insurance, the legal person's certificate of registration, legitimate proof of the authority of the person purporting to act on behalf of the customer (such as a business license, other incorporation or license of registration, etc.), and the identification documents, data or information of the holding or controlling beneficial owner of the legal person should be provided or the information thereon should be recorded. A solicitor should make remark on the solicitation report after validating identification information on the insurance application form.

ii. An underwriter should review the application forms filled out by the applicant or the insured at the time of underwriting with due diligence to ensure that the CDD made on the parties hereof in the solicitation report is true. If necessary, an underwriter should request a survival investigation on the application case and attach relevant information for recordation. When a legal person is applying for insurance, an insurance company should take reasonable methods to understand the nature of its business, the beneficial owner and the control structure, and keep relevant documents and information.

iii. In addition to identification card and license of registration, a second identification document should be requested for the CDD, if necessary. The second identification document should be identity-provable. A name list issued by organizations, schools or groups can also be used as a second identification documents if it can serve as confirmation of a party's identity. If the parties hereof refuse to provide a second identification documents herein, the application should be declined or be processed after the CDD is completed.

iv. An insurance purchased by any person acting on behalf of a customer should follow Item 2 of Subparagraph 3 herein.

(2) An insurance company should adopt the following measures when the beneficiary(ies) of a life insurance policy, investment-linked insurance policy or annuity insurance policy have been identified or designated:

i. Obtaining the name and identification document number or registration (incorporation) date of the designated beneficiary.

ii. For beneficiary(ies) that are designated by contract characteristics or by other means, obtaining sufficient information concerning the beneficiary to satisfy the insurance company that it will be able to establish the identity of the beneficiary at the time of the payout.

(3) Directions for Verifying Customer Information of Written Cases

i. When a customer of a jumbo case (the amount is subject to each company's discretion) cancels a policy from inception and asks for refund of premium paid, an insurance company should initiate a project to process the case and the verify the identity and the motive of the customer to prevent money laundering or terrorist financing activities.

ii. An insurance company should understand an individual customer's occupation and residence or a legal person customer's business location and business nature via telephone, letter or other means, if necessary, and keep the relevant information.

iii. If irregularities arise when the customer applies for policy loan, policy change, such as change of premium-payment method, applicant or beneficiary, etc., or policy surrender, an insurance company should pay close attention to such applications and proceed further review.

iv. A policy change made by any person acting on behalf of a customer should follow Item 2 of Subparagraph 3 herein.

(4) Directions for Claims Payment

i. An insurance company should verify the identity of the beneficiary(ies) of a life insurance policy, investment-linked insurance policy or annuity insurance policy at the time of payout.

ii. When paying out insurance proceeds, an insurance company should review the payment flow if any suspicion arises. If the beneficiary demands to cancel "non-negotiable" remark off the check, an insurance company should understand the motive, and makes adequate notes.

iii. An insurance company should review whether the process of changing of beneficiary is normal and reasonable.

iv. An insurance company should review whether there is a reasonable connection between the amount of insurance proceeds and the beneficiary's occupation or identity.

v. Claims application made by any person acting on behalf of a customer should follow Item 2 of Subparagraph 3 herein.

(5) Where an insurance company is unable to complete the required CDD process on a customer, it should consider filing an STR in relation to the customer.

(6) If an insurance company forms a suspicion that a customer or a transaction relates to money laundering or terrorist financing and reasonably believes that performing the CDD process will tip-off the customer, it may choose not to pursue that process, and should file an STR.

(7) For a non-face-to-face customer, an insurance company should perform CDD procedures that are as effective as those performed in the ordinary course of business and must include special and sufficient measures to mitigate the risks.

(8) For a customer establishing business relationship with an insurance company through the internet, the insurance company should follow relevant model operating procedures developed by the Life Insurance Association of the Republic of China ("LIA") and approved by regulators.

15. In the case that a customer in a business relationship or transaction is described in Item 8 of Subparagraph 8, an insurance company should file an STR report in accordance with Article 10 of the Money Laundering Control Act. If such a customer is a designated individual or entity

sanctioned under the Terrorism Financing Prevention Act, an insurance company is prohibited from the activities described in Paragraph 1 of Article 7 of the Terrorism Financing Prevention Act since the date of knowledge, and should report in accordance with Article 12 of the Terrorism Financing Prevention Act (please download the reporting format on the website of the Investigation Bureau, Ministry of Justice). If an insurance company is involved in the activities described in the Subparagraph 3 and 4 of, Paragraph 1 of Article 6 of Terrorism Financing Prevention Act before aforementioned individuals or entities are listed as designated individuals or entities, an insurance company should obtain the approval of Terrorism Financing Prevention Committee in accordance with relevant regulations established under Terrorism Financing Prevention Act.

Article 5

The CDD measures of an insurance company should include ongoing customer due diligence and observe the following requirements:

1. An insurance company should apply CDD requirements to existing customers on the basis of materiality and risk, and conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained. The aforementioned appropriate times include at least:

   (1) When the customer increases the sum assured irregularly or enters new business relationships with the insurance company.

   (2) When it is time for periodic review of the customer scheduled on the basis of materiality and risk.

   (3) When it becomes known that there is a material change to customer's identity and background information.

2. An insurance company should conduct ongoing due diligence on the business relationship to scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with its knowledge of the customer and its business and risk profile, including, where necessary, the source of funds.

3. An insurance company should periodically review the existing records to ensure that documents, data or information of the customer and its beneficial owner(s) collected under the CDD process are kept up-to-date and relevant, particularly for higher risk customers, whose reviews should be conducted at least once every year. The frequency for reviewing all other customers should be based on a risk-based approach.

4. An insurance company can rely on existing customer records to undertake due diligence. Therefore, an insurance company is allowed to carry out transactions without repeatedly identifying and verifying the identity of an existing customer. However, an insurance company should conduct CDD measures again in accordance with Article 4 herein if it has doubts about the veracity or adequacy of the records, such as, where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

Article 6

An insurance company should determine the extent of applying CDD measures under Subparagraph 3 of Article 4 using a risk-based approach (RBA), including:

1. For higher risk situations, an insurance company should perform enhanced CDD or ongoing due

diligence measures by adopting at least the following enhanced measures:

(1) An insurance company should obtain approval from the senior management determined according to the insurance company's internal consideration of risk before establishing or entering into new business relationships.

(2) An insurance company should take reasonable measures to understand the sources of wealth and the source of funds of the customer. The source of funds refers to the original source that generates such funds (e.g. salary, investment proceeds, disposal of real estate, etc.)

(3) An insurance company should conduct enhanced ongoing monitoring of business relationship.

2. For customers from high-risk countries or territories known to have inadequate AML/CFT regimes, an insurance company should conduct Enhanced Due Diligence measures consistent with the risks identified.

3. For lower risk circumstances, an insurance company may apply simplified CDD measures, which should be commensurate with the lower risk factors. However, simplified CDD measures are not allowed in any of the following circumstances:

(1) Where customers are from countries or territories known to have inadequate AML/CFT regimes, including but not limited to those forwarded by the FSC to have been designated by international organizations as countries or territories with serious deficiencies in their AML/CFT regimes, and other countries or territories that do not follow or insufficiently follow the recommendations of international organizations.

(2) Where there is a suspicion of money laundering or terrorist financing in relation to the customer or the transaction.

An insurance company may adopt the following simplified CDD measures:

1. Reducing the frequency in updating the customer identity information.

2. Reducing the level of ongoing monitoring and use reasonable threshold amount as a basis for review on transactions.

3. If the purpose and nature of business can be inferred based on the type of transaction or the established business relationship, it is not necessary to re-collect specific information or implement special measures to understand the purpose and nature of the business relationship.

An insurance company should apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

An insurance company should consider the beneficiary of a life insurance policy as a relevant risk factor in determining whether to apply Enhanced Due Diligence measures. If the insurance company determines that a beneficiary who is a legal person or a trustee presents a higher risk, the Enhanced Due Diligence measures should include reasonable measures to identify and verify the identity of the actual beneficiary before making benefit payout.

Article 7

An insurance company should perform its own CDD measures. However, if it is otherwise permitted by law or the FSC that an insurance company may rely on a third party to perform the identification and verification of the identities of customers, agents and beneficial owners or the purpose and intended nature of the business relationship, the insurance company relying on the third party should

still bear the ultimate responsibility for CDD measures and observe the following requirements:

1. An insurance company relying on a third party should be able to immediately obtain the necessary CDD information.
2. An insurance company should take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
3. An insurance company should make sure that the third party it relies on is regulated, supervised or monitored, and has appropriate measures in place for compliance with CDD and record-keeping requirements.
4. An insurance company should make sure that the jurisdiction where the third party it relies on is located has AML/CFT regulations in place that are consistent with the standards set out by the FATF.

Article 8

An insurance company should observe the following requirements in name screening of customers and related parties of a transaction:

1. An insurance company should establish policies and procedures for name screening of customers and related parties of a transaction, using a risk-based approach, to detect, match and filter whether customers, or the senior managerial officers, beneficial owners or related parties of a transaction are individuals, legal persons or organizations sanctioned under the Terrorism Financing Prevention Act or a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization. The matched customer should be processed pursuant to Paragraph 15 of Article 4 herein.
2. The policies and procedures for name screening of customers and related parties of a transaction should include at least matching and screening logics, implementation procedures and evaluation standards, and should be documented.
3. An insurance company should document its name screening operations and maintain the records for a time period in accordance with Article 13 herein.
4. The name screening mechanism should be subject to testing, including:
   (1) Whether the sanction list and threshold setting are determined by applying a risk-based approach.
   (2) Whether the mapping between data input and system data field is correct and complete.
   (3) The logic of matching and screening.
   (4) Model validation.
   (5) Whether data output is correct and complete.
5. An insurance company should determine whether such mechanism continues to appropriately reflect the risk identified and update the mechanism at proper time.

Article 9

An insurance company should observe the following requirements for ongoing monitoring of transactions:

1. An insurance company should step by step use a database to consolidate basic information and transaction information on all customers for inquiries by the head office and branches for AML/CFT purpose so as to strengthen its capability of transaction monitoring. An insurance company should also establish internal control procedures for requests and inquiries as to customer information made by various units and should exercise care to ensure the confidentiality of the information.

2. An insurance company should establish policies and procedures for transaction monitoring using a risk-based approach and utilize information system to assist in the detection of suspicious money laundering and terrorist financing transactions.

3. An insurance company should review its policies and procedures for transaction monitoring based on AML/CFT regulations, nature of customers, business size and complexity, money laundering and terrorist financing trends and related information gathered from internal and external sources, and its risk assessment results, and update those policies and procedures periodically.

4. The policies and procedures for transaction monitoring of an insurance company should include at least the complete money laundering and terrorist financing monitoring indicators, and carrying out the setting of parameters, threshold amounts, alerts and monitoring operations, the procedures for examining the monitored cases and reporting standards, and should be documented.

5. The mechanism provided in the preceding subparagraph should be subject to testing, including:

   (1) Internal control procedure: review the roles and responsibilities of persons or business units related to the mechanism for monitoring transactions.

   (2) Whether the mapping between data input and system data field is correct and complete.

   (3) The logic of detection scenario.

   (4) Model validation.

   (5) Data output.

6. In the cases where an insurance company identifies or has reasonable grounds to suspect customers, or the funds, assets or intended or performed transactions of the customers are related to money laundering and terrorist financing, regardless of the amount, value, or whether transactions are completed, an insurance company should perform enhanced review of the customer identity.

7. The red flags for suspicious money laundering and terrorist financing transactions provided in the Appendix are not exhaustive. An insurance company should select or develop suitable red flags based on its size of assets, geographic areas, business profile, customer base profile, characteristics of transactions, and the insurance company's internal money laundering and terrorist financing risk assessment or information of daily transactions, to identify red flag transactions of potential money laundering and terrorist financing.

8. For red flag transactions identified in accordance with the preceding subparagraph, an insurance company should determine whether such transactions are reasonable (e.g. whether such transactions are apparently incommensurate with the identity, income, or scale of business of the customer, are unrelated to the customer's business profile, do not match the customer's business model, or are without reasonable economic purpose, reasonable explanation, reasonable purpose, or clear source of funds or explanation) and keep review records. If an insurance company determines such transaction is not a suspicious money laundering and terrorist financing transaction, the insurance company should record the reason for the decision. If an insurance company determines such transaction is suspicious money laundering and terrorist financing transaction, in addition to performing CDD measures and retaining relevant documentations, the

insurance company should report to the Investigation Bureau, Ministry of Justice within 10 business days since such transaction is identified and confirmed as a suspicious money laundering and terrorist financing transaction.

9. With respect to red flags for suspicious money laundering and terrorist financing transactions, an insurance company should determine the ones that are required to be monitored with the assistance of related information systems by applying a risk-based approach. For those that are monitored without the assistance of information systems, an insurance company should also, by other means, assist employees to determine whether transactions are suspicious money laundering and terrorist financing transactions when they are processed by customers. The assistance of information system cannot replace the judgment of employees. An insurance company is still required to strengthen employee training to allow employees capable of identifying suspicious money laundering and terrorist financing transactions.

Reporting of suspicious money laundering and terrorist financing transactions:

1. When an employee of a business unit identifies any abnormal transaction, the employee should immediately report such transaction to a supervisory officer.

2. The supervisory officer should determine as soon as possible whether such transaction is subject to reporting requirements. If it is determined that such transaction should be reported, the supervisory officer should immediately request the employee to complete a report (please download the reporting format on the website of the Investigation of Bureau, Ministry of Justice).

3. After the report is approved by the head of the business unit, an insurance company should submit the report to the responsible unit.

4. After the report is submitted by the responsible unit and approved by AML/CFT Officer, an insurance company should file the report immediately to the Investigation of Bureau, Ministry of Justice.

5. In the case of an apparently significant and urgent suspicious money laundering and terrorist financing transaction, an insurance company should immediately report to the Investigation of Bureau, Ministry of Justice by fax or other feasible means and then immediately submit the hard copy of the report. An insurance company is not required to submit the hard copy of the report, provided that the Investigation of Bureau, Ministry of Justice confirms the receipt of such report by sending a fax reply. In addition, an insurance company should retain the fax reply.

Requirements on the confidentiality of reporting data and information are as follows:

1. Employee at all levels should keep the reporting of suspicious money laundering and terrorist financing transactions confidential and should not disclose such information. An insurance company should provide employees trainings or materials on how to avoid the disclosure of such information in the interaction with customers and in daily operation.

2. All documents related to such reporting should be classified as confidential. In the cases of any disclosure, an insurance company should take measures in accordance with relevant requirements.

3. The AML/CFT employees, compliance employees or internal auditors should be able to timely obtain customer identification data and transaction records of a customer for the purpose of perform their duties, provided that the confidentiality requirements are followed.

An insurance company should record the result of ongoing transaction monitoring and keep such record in accordance with the requirements of Article 13.

Article 10

An insurance company should assess the money laundering and terrorist financing risks before launching new products, services, or new businesses (including new delivery mechanisms, use of new technologies for existing or new products or businesses) and establish relevant risk management measures to mitigate the identified risks.

Article 11

An insurance company should observe the following requirements with respect to cash transactions above a certain amount:

1. An insurance company should verify the identity of the customer and keep relevant transaction records.

2. An insurance company should conduct CDD measures in accordance with the following requirements:

   (1) An insurance company should verify customer identity with the identification documents or the passport provided by the customer, and record the name, date of birth, address, telephone number, account number where the account is used to process the transaction, transaction amount, and identification number of the customer. In case where the customer is the owner of the account used to process transactions, however, an insurance company may not verify the identity but describe the transaction is processed by the account owner on transaction records.

   (2) In case where the transaction is processed by a person acting on behalf of the customer, an insurance company should verify the person's identity with the identification documents or the passport provided by the person, and record the name, date of birth, address, telephone number, account number where the account is used to process transactions, transaction amount, and identification number of the person.

3. Except for situations specified in Paragraph 2 and 3 herein, an insurance company should report such transactions within 5 business days after the completion of transactions in the way of media reporting (please download the format on the website of the Investigation of Bureau, Ministry of Justice) to the Investigation of Bureau, Ministry of Justice. In case where an insurance fails to complete media reporting with a justified reason, it may submit a hard copy of the report after obtaining the consent from the Investigation of Bureau, Ministry of Justice.

4. An insurance company should keep the data reported to the Investigation Bureau and relevant transaction records in accordance with Article 13 herein.

An insurance company is not required to file a report on any of the following cash transactions above a certain amount with the Investigation Bureau, but remains required to conduct CDD and keep the transaction records thereof:

1. Payments deposited into an account opened by a government, a government-owned enterprise, an entity commissioned to exercise public authority (within the scope of commission), a public or private school, a public utility, and a fund established by a government in accordance with applicable regulatory requirements.

2. Transactions and fund arrangements between financial institutions. Notwithstanding the foregoing, payables to another financial institution's customer paid through an inter-bank deposit account, such as a customer cashing the check issued by another financial institution, should be handled as required, provided the cash transaction of a customer is above a certain amount.

3. Payments collected on behalf of a third party (excluding payments deposited in designated stock subscription accounts and credit card payments collected) where the payment notices expressly

bear the name and identification card number of the transaction party's name (including the code which enables tracking of the transaction party's identity), and the type and amount of the transactions. Nevertheless, the duplicate copies of the payment notices should be kept as transaction records.

In case of non-individual accounts such as those opened by department stores, wholesale stores, supermarket chains, gas stations, hospitals, transportation businesses and hotels and restaurants which must deposit cash amounting to over a certain amount constantly or routinely in line with business needs, a financial institution may, after verifying the actual business needs, submit the name list to the Investigation Bureau for recordation. Verification and reporting of transactions on a case-by-case basis may be waived for such an account unless the Investigation Bureau responds to the contrary within ten (10) days from the receipt of the name list.

An insurance company should examine the counterparties to the transactions exempted from reporting on a case-by-case basis at least once every year, and report to the Investigation Bureau for recordation if a transaction party no longer has business dealing as mentioned in this paragraph with it.

If any suspicious money laundering and terrorist financing transaction is discovered in the transactions mentioned in the preceding two paragraphs, it is still pursuant to the requirements in Article 10 of the Money Laundering Control Act and Paragraph 2, Article 7 of the Terrorism Financing Prevention Act.

Article 12

An insurance company should report on the properties or property interests and location of the person sanctioned under Article 7 of the Terrorism Financing Prevention Act in accordance with the following requirements:

1. Within ten business days upon discovery of a suspicious money laundering and terrorist financing transaction, an insurance company should promptly file a report with the Ministry of Justice Investigation Bureau in a format prescribed by the Bureau after the report has been approved by the Chief AML/CFT Officer of the insurance company.

2. If the reporting mentioned in the preceding paragraph is of obvious and significant urgent nature, an insurance company should file the reporting as soon as possible to the Investigation Bureau by fax or other available means and follow it up with a written report. An insurance company is not required to submit a follow-up written report, provided the Investigation Bureau has acknowledged the receipt of report by sending a reply by fax. In such event, an insurance company should keep the faxed reply.

3. An insurance company should set December 31 of each year as the base date of settlement to prepare, in accordance with the format set out by the Ministry of Justice Investigation Bureau, an annual report documenting all properties or property interests held by the individuals, legal persons or organizations sanctioned under Article 7 of the Terrorism Financing Prevention Act that are managed by the insurance company, and submit to the Ministry of Justice Investigation Bureau for recordation before March 31 of the following year.

The preceding reporting records, proof of transaction and annual report should be handled in accordance with the requirements set out in Article 13 herein.

Article 13

An insurance company should keep records on all business relations and transactions with its customers in hard copy or electronical form and in accordance with the following requirements:

1. An insurance company should maintain all necessary records on transactions, both domestic and international, for at least five years or a longer period as otherwise required by law. The aforementioned necessary records including:

   (1) Name or account number or identification document number of each transaction party.

   (2) Transaction date.

   (3) Currency type and amount.

   (4) Payment methods, such as cash, checks and so on.

   (5) Destination of payments.

   (6) Instruction or authorize method.

2. For currency transactions above a certain amount, an insurance company should keep relevant records on the verification and reporting of such transactions for at least 5 years in the original manner. For ways to record the information obtained through the CDD procedures, an insurance company may determine a way to record such information based on its own consideration and the principle of consistency across the entire insurance company.

3. For the reporting of a suspicious money laundering and terrorist financing transactions, an insurance company should keep relevant records of reporting for at least 5 years in the original manner.

4. An insurance company should keep following information for at least 5 years after the business relationship is ended or a longer period as otherwise required by law.

   (1) All records obtained through CDD measures, such as photocopies or records of official identification documents like passports, identity cards, driving licenses or similar documents.

   (2) Contract files.

   (3) Business correspondence, including inquiries to establish the background and purpose of complex, unusual transactions and the results of any analysis undertaken.

5. Transaction records maintained by an insurance company must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity

6. An insurance company should ensure that transaction records and CDD information will be available swiftly to the competent authorities when such requests are made with appropriate authority.

Article 14

Other Directions that Require Attention:

1. An insurance company should pay attention when a customer or solicitor is suspected of circumventing the requirements of Money Laundering Control Act (such as the same applicant or the insured separately purchases a jumbo insurance), and ensure its motives are understood.

2. An insurance company should review its internal control measures annually (the time is subject to each insurance company’s discretion) to see if it is adequate to prevent money laundering and terrorist financing behaviors. If there is any deficiency in the operation of each unit, it should be promptly improved.

3. An insurance company should pay attention on confidentiality when investigating any employee (staff) suspected of involvement in money laundering or terrorism financing.

Article 15

Dedicated AML/CFT unit and Chief AML/CFT Officers:

1. An insurance company should be staffed with adequate number of AML/CFT personnel and resources appropriate to the size and risks of its business. The board of directors（council） of the insurance enterprise should appoint a senior officer to act as the Chief AML/CFT Officer and vest the officer full authority in coordinating and supervising AML/CFT implementation and should ensure that its AML/CFT personnel and the Chief AML/CFT Officer do not hold concurrent positions that may have a conflict of interest with their AML/CFT responsibilities. A domestic life insurance company should set up an independent, dedicated AML/CFT compliance unit under the general manager, the head office compliance unit or risk management unit of the head office. The AML/CFT unit may not handle businesses other than AML/CFT.
2. The dedicated AML/CFT unit or Chief AML/CFT Officer mentioned in the preceding subparagraph should be charged with the following duties:
   (1) Supervising the planning and implementation of policies and procedures for identifying, assessing and monitoring money laundering and terrorist financing risks.
   (2) Coordinating and supervising company-wide AML/CFT risk identification and assessment.
   (3) Monitoring and controlling money laundering and terrorist financing risks.
   (4) Developing an AML/CFT program.
   (5) Coordinating and supervising the implementation of AML/CFT program.
   (6) Confirming compliance with AML/CFT regulations, including the relevant compliance template or self-regulatory rules produced by the LIA and approved by the FSC.
   (7) Supervising the report on transactions suspicious of money laundering or terrorist financing and on the properties or property interests and location of individuals or legal entities designated by the Terrorism Financing Prevention Act to the Investigation Bureau, Ministry of Justice.
   (8) Other matters relating to AML/CFT.
3. The Chief AML/CFT Officer mentioned in Subparagraph 1 hereof should report to the board of directors and supervisors (board of supervisors) or audit committee at least every half year. If any significant non-compliance is identified, the Chief AML/CFT Officer should immediate report to the board of directors and supervisors (board of supervisors) or audit committee.
4. A foreign business unit of an insurance company should deploy adequate and sufficient AML/CFT personnel by taking into account the number of local branches, size of business, risks, etc. and appoint a head responsible for supervising AML/CFT affairs
5. The appointment of AML/CFT head of an insurance company's foreign business unit should meet local regulatory regulations and the requirements of local competent authorities. The head should be sufficiently authorized to coordinate AML/CFT affairs, including that the head may directly report to the Chief AML/CFT Officer described in Subparagraph 1, and should not take other responsibilities except compliance head. In case where the head may take other responsibilities, an insurance company should discuss with local competent authorities to ensure such arrangement has no concern in conflict of interest and report to FSC for recordation.

Article 16

Implementation, audit and statement of internal AML/CFT control system:

1. A domestic and foreign business unit of an insurance company should appoint a senior manager to act as the supervisor to take charge of supervising AML/CFT related matters of the business unit, and conduct self-inspection in accordance with relevant rules.

2. The internal audit unit of an insurance company should audit the following matters in accordance with the regulations and provide audit opinions:

   (1) Whether the money laundering and terrorist financing risk assessment and the AML/CFT program meet the regulatory requirements and are vigorously implemented.

   (2) The effectiveness of AML/CFT program.

3. Responsibilities of the internal audit unit of an insurance company:

   (1) Establishing audit plans in accordance to relevant internal control measures, conducting periodic audit, and testing the effectiveness of AML/CFT programs and risk management quality of operations, departments and branches (or subsidiaries).

   (2) The auditing should cover independent transaction testing, including selecting transactions related to high-risk products, customers, and geographic areas to verify that an insurance company has effectively implemented relevant AML/CFT regulatory requirements.

   (3) In case where any deficiency in the implementation of specific management measures is identified, internal audit unit should periodically report to the Chief AML/CFT Officer for review and provide such information as a reference of employee training.

   (4) In case where internal audit unit identifies any intentional disguise of significant non-compliance but fails to disclose such information, head office competent unit should take appropriate actions.

4. The general manager of an insurance company should oversee that respective units prudently evaluate and review the implementation of internal AML/CFT control system. The chairman of the board (chairman of the council), the general manager, the Chief Internal Auditor (internal auditor) and the Chief AML/CFT Officer should jointly issue a statement on internal AML/CFT control, which should be submitted to the board of directors (council) for approval and disclosed on the website of the insurance company within three months after the end of each fiscal year, and filed via a website designated by the FSC.

5. For the branches of a foreign insurance enterprise in Taiwan, the authorized person of its head office should be responsible for matters concerning the board of director or supervisors under the model policy and procedure. The statement mentioned in the preceding subparagraph should be jointly issued by the responsible person and the Chief AML/CFT Officer of the branch in Taiwan as authorized by the head office as well as officer in charge of audit operation in Taiwan.

Article 17

Employee hiring and training:

1. An insurance company should establish proper and appropriate procedures for employee screening and hiring, including examining whether the prospective employee has character integrity and the professional knowledge required to perform their duties.

2. The Chief AML/CFT Officer, the personnel of dedicated AML/CFT unit and the AML/CFT

supervisory officer of domestic business units of an insurance company should possess one of the following qualification requirements in three months after appointment/assignment to the post and the insurance company should set out relevant control mechanism to ensure compliance with the requirements hereof:

(1) Having at least 3-year experience as compliance or AML/CFT personnel.

(2) For the Chief AML/CFT Officer and personnel of dedicated AML/CFT unit, having attended not less than 24 hours of courses offered by institutions recognized by the FSC, passed the exams and received completion certificates therefor; for the AML/CFT supervisory officers of domestic business units, having attended not less than 12 hours of courses offered by institutions recognized by the FSC, passed the exams and received completion certificates thereof. But the Chief AML/CFT Officers who also act as the Chief Compliance Officer or personnel of dedicated AML/CFT unit who also acts as compliance personnel are deemed to meet the qualification requirement under this item after they have attended at least 12 hours of training on AML/CFT offered by institutions recognized by the FSC.

(3) Having received a domestic or international AML/CFT professional certificate issued by an institution recognized by the FSC.

3. Personnel mentioned in the preceding subparagraph who are appointed/assigned to the post prior to August 31, 2017 may be deemed as qualified if he or she meets any of the qualification requirements below:

   (1) Meeting the qualification requirement set out in Item 1 or Item 3 of the preceding subparagraph prior to August 31, 2017.

   (2) Meeting the qualification requirement set out in Item 2 of the preceding subparagraph within the time periods specified below:

      i. For the Chief AML/CFT Officer and AML/CFT personnel, meeting the qualification requirement within six months after appointment /assignment to the post.

      ii. For AML/CFT supervisory officers of domestic business units, meeting the qualification requirement within one year after appointment/assignment to the post.

4. The Chief AML/CFT Officer, the personnel of dedicated AML/CFT unit and the AML/CFT supervisory officers of domestic business units of an insurance company should attend not less than 12 hours of training on AML/CFT offered by internal or external training units consented by the Chief AML/CFT Officer mentioned under Paragraph 1 of Article 15 herein every year. The training should cover at least newly amended laws and regulations, trends and patterns of money laundering and terrorist financing risks. If the person has obtained a domestic or international AML/CFT professional certificate issued by an institution recognized by the FSC in a year, the certificate may be used to offset the training hours for the year.

5. The AML/CFT supervisory officers and the AML/CFT officer and personnel of foreign business units of an insurance enterprise should possess professional knowledge in AML/CFT, be well informed in relevant local regulations, and attend not less than 12 hours of training on AML/CFT offered by foreign competent authorities or relevant institutions every year. If no such training is available, the personnel may attend training courses offered by internal or external training units consented by Chief AML/CFT Officer mentioned under Paragraph 1 of Article 15 herein.

6. An insurance company should arrange appropriate hours of training of suitable contents on AML/CFT every year in view of the nature of its business for its directors (council members), supervisors, general manager, compliance personnel, internal auditors, sales agents and personnel related to AML/CFT operation to familiarize them with their AML/CFT duties and equip them

with the professional knowhow to perform their duties.

7. An insurance company should arrange AML/CFT-related on-the-job training courses for the internal and external employees at all levels so that all employees understand the relationship between the relevant laws and regulations regarding AML/CFT risks and the practical operations. And, if necessary, scholars from the Ministry of Justice, the FSC, colleges and universities or other organizations should be hired as lecturers.
8. An insurance company's employees should take advantage of the opportunity to learn about the AML/CFT practices in foreign life insurance sector when they go abroad for further studies or surveys, and should be rewarded on a case-by-case basis if they can provide sufficient references on a method for the company to adopt.

Article 18

If a customer meets the following situations, the service should be declined and report to the supervisor directly:

1. Insisting not to provide relevant data for identity verification when being told it is necessary according to legal or regulatory requirements.
2. Any individuals or entities compel or attempt to compel an insurance company's employees not to file transaction records or reporting forms.
3. Attempting to persuade employees not to collect data that is required to complete the transaction.
4. Enquiring the possibility of avoiding being reported.
5. Eager to explain the source of fund is clean or the transaction is not for money laundering purpose.
6. Insisting transactions must be completed immediately without a reasonable explanation.
7. Descriptions provided by the customers apparently do no match the transactions.
8. Attempting to provide interest to employees to obtain services provided by an insurance company.

Article 19

An insurance company should stipulate in the joint-promotion distribution agreement, the cross-selling agreement, insurance agent agreement, or the insurance broking agreement with an insurance agent company or an insurance broker company that the insurance agent company or insurance broker company should follow the AML/CFT regulations and cooperate with the insurance company in the collection or verification of the customer identification data.

An insurance company should demand and confirm with the insurance agent company or insurance broker company hereof to fully cooperate in the AML/CFT matters during business solicitation.

Article 20

An insurance company should establish its own Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism ("Directions") by reference to the Model Guidelines and implement the Directions after obtaining approval from the board of directors (council). An insurance company should report the Directions to the FSC and perform annual review of the Directions. In the case of amending the Directions, the requirements of this Article also apply.

Article 21

The Model Guidelines and any subsequent amendment thereto should be authorized by council of the LIA and report to the FSC for recordation after the implementation.

Appendix:
Types of Suspicious Money Laundering or Terrorist Financing Transactions

Attachment:
Guidelines for Insurance Companies Regarding Assessment of Money Laundering and Terrorism Financing Risks and Adoption of Prevention Programs