Model Guidelines for Non-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 set up 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 established in accordance with "Implementation Rules of Internal Audit and Internal Control System of insurance Industries" and its amendment should be approved by the board of directors. Such internal control systems should include:

I. Policies and procedures for identifying, assessing, and managing the risk of money laundering and terrorism financing ("ML/TF") established in accordance with "Guidelines to Insurance Companies on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program" ("Guidelines"). See attachment.

II. Anti-money laundering and countering the financing of terrorism ("AML/CFT") programs established in accordance with the Guidelines and based on risk assessment result and scale of business to manage and mitigate the risks identified and take enhanced control measures with respect to higher risk categories.

III. Procedures for supervising the compliance of AML/CFT regulations and the implementation of AML/CFT programs. Such procedures, subject to self-inspection and internal audit, should be enhanced if necessary.

The identification, assessment and management of ML/TF risks provided in subparagraph I of last paragraph should at least cover the aspect of customers, geographic areas, and products, services, transactions or delivery channels, etc. In addition, an insurance company should comply with following rules:

I. Generating a risk assessment report.

II. Considering all risk factors to determine the insurance company's level of risk and the appropriate measures to mitigate risks.

III. Having a mechanism in place for updating risk assessment report periodically to ensure the update of risk profile.

IV. Filing the risk assessment report to Financial Supervisory Commission ("FSC") after it is completed or updated.

The AML/CFT programs provided in subparagraph II of paragraph 1 should include following policies, procedures and controls:

I. Customer due diligence ("CDD")

II. Name screening on customers and related parties of a transaction.

III. Ongoing monitoring of accounts and transactions.

IV. Record-keeping.

V. Reporting of currency transactions that reach a certain amount.

VI. Reporting of suspicious ML/TF transactions and reporting in accordance with "Counter-Terrorism Financing Act".

VII. Appointment of an AML/CFT responsible officer.

VIII. Procedures for screening and hiring employees.

IX. An ongoing employee training program.

X. An independent audit function to test the effectiveness of AML/CFT system.

XI. Others required in AML/CFT related regulations or by FSC.

An insurance company that has any foreign branch (or subsidiary) should establish group-level AML/CFT programs and implement such programs in all branches and subsidiaries. In addition to the policies, procedures and controls provided in last paragraph, on condition that the regulatory requirements on data confidentiality of R.O.C. and jurisdictions where the insurance company has any foreign branch (or subsidiary) are met, such programs should include:

I. Policies and procedures for sharing information within the group required for the purposes of CDD and ML/TF risk management.

II. That group-level compliance, audit, and AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes.

III. Safeguards on the confidentiality and use of information exchanged.

An insurance company should ensure its foreign branches (or subsidiaries) implement the AML/CFT measures of head office (or parent company) on condition that local regulatory requirements are met. In the case that regulatory requirements of the jurisdictions where head office (or parent company) and a branch (or subsidiary) are located are different, the branch (or subsidiary) should comply with the stricter ones. If there are any doubts in determining whether regulatory requirements are stricter or less strict, an insurance company should follow the determination of competent authorities in the jurisdiction where the insurance company's head office (or parent company) is located. If an insurance company's branch (or subsidiary) is not allowed to implement the measures of head office (or parent company) due to conflicting with foreign regulatory requirements, the insurance company should apply appropriate additional measures to manage ML/TF risks and inform FSC.

For any branch or subsidiary of a foreign financial group in Taiwan, with respect to the policies and procedures for identifying, assessing and managing ML/TF risks and the policies, procedures, and controls that AML/CFT programs should include, provided in subparagraph I and II of paragraph 1 and established in accordance with the Guidelines, 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 of an insurance company takes the ultimate responsibility for ensuring the establishment and maintenance of appropriate and effective AML/CFT internal controls. The board of directors and senior management should understand the insurance company's ML/TF risks and the implementation of AML/CFT programs, and take measures to form a strong AML/CFT culture.

Article 3

The terms used in the Model Guidelines are defined as follows:

I. "A certain amount" refers to TWD 500,000 (or equivalent foreign currency).

II. "Currency transaction" refers to receiving cash or paying cash in a single transaction (including any transaction that is recorded on a cash deposit or

withdrawal slip for accounting purpose)

III. "Establishing business relationship" means that a person requests an insurance company to provide financial services and establish relationship that can continue for a duration, or that a person first approaches an insurance company as a potential customer and expects such relationship that may continue for a duration.

IV. "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)

V. "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.

VI. "Risk-based approach" refers to that an insurance company should identify, assess and understand the ML/TF 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 risk scenarios while simplified measures may be taken for lower risk scenarios to effectively allocate resources and mitigate the identified ML/TF risks in the most appropriate and effective way.

VII. "Related parties of a transaction" refer to any third party, which is other than an insurance company's customers, involved in a transaction,

Article 4

An insurance company should comply with following requirements when conducting CDD measures:

I. An insurance company should avoid establishing business relationship or processing transactions if any of following scenarios is identified:

(i) A customers is suspected to use anonymous, fake name, figurehead, fictitious business or entity.

(ii) A customer refuses to provide relevant documentations required for the purpose of CDD except that an insurance company may verify the client's identify using reliable, independent source of information.

(iii) 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.

(iv) Using counterfeit or altered identity documents.

(v) Identification documents presented are hard copies except for the business that permits the use of hard copies or soft copies of identification documents with other alternative measures under applicable regulations.

(vi) The relevant documentations provided are suspicious blurred and indistinct. Clients refuse to provide other documents to prove, or those documents are unable to be reviewed.

(vii) A customer delays in providing of required customer identification documents in an unusual manner.

(viii) The parties with whom an insurance company establishes business relationship are designated individuals or entities sanctioned under Counter-Terrorism Financing Act and terrorists or terrorist groups that are identified or investigated. This requirement, however, does not apply to any payment made in accordance with subparagraph II to IV of paragraph 1 of Article 6 of "Counter-Terrorism Financing Act".

(ix) Other unusual scenarios occur when an insurance company establishes business relationship with or processes transactions for a customer and the customer fails to provide a reasonable explanation.

II. An insurance company should perform CDD when:

(i) Establishing business relationship with a customer.

(ii) Carrying out transactions above NT$500,000 (or equivalent foreign currency), including receiving cash or paying cash in a single transaction (including any transaction that is recorded on a cash deposit or withdrawal slip for accounting purpose).

(iii) Identifying a suspicious ML/TF transaction.

(iv) It has doubts about the veracity and adequacy of previously obtained customer identification data.

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

(i) Identifying the customer and verifying the customer identity using reliable, independent source documents, data or information, and retaining hard copies of customer identity documents or recording the relevant information thereon.

(ii) In the case that any person acts on behalf of a customer to establish business relationship or conduct 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 subparagraph III.(i), and retain hard copies of the agent's identity documents or record the relevant information thereon.

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

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

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

(i) Name;

(ii) Date of birth;

(iii) Household registration or residence address;

(iv) Official identification number;

(v) Nationality; and

(vi) The purpose of application for insurance by a foreign person .

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

(i) The name, legal form, and proof of existence of the customer or trust;

(ii) The articles of incorporation or similar powers that regulate and bind the entity or trust except in following circumstances:

1. The entity or trust is one of entities provided in subparagraph VI.(iii) without any circumstances provided in Subparagraph III.(i) and (ii) of Paragraph 1 of Article 6.
2. The entity customer confirmed has no articles of incorporation or

similar powers;

(iii) Following information of persons holding the position of senior management (including directors, supervisors, chief executive officer, chief financial officer, authorized representatives, temporary manager, partners, authorized signatories, or any natural person having equivalent aforementioned position, an insurance company should determine the scope of senior management position by applying a risk-based approach).

(iv) Registered address and main business addresses of an entity or trustee of a trust; and

VI. For a customer that is an entity or trustee of a trust, an insurance company, when applying the requirements under subparagraph III.(iii), should understand the ownership and control structure of the customer, and identify the beneficial owner of the customer and take reasonable measures to verify the identity of such persons through following information:

(i) For a customer that is an entity:

1. The identity of the natural person(s) who ultimately has a controlling ownership interest in an entity (such as name, date of birth, nationality, and identification number, etc.) "Natural person(s) who ultimately have a controlling ownership interest in an entity" refers to any natural person that directly or indirectly owns more than 25 percent of shares or capital of the entity. In such case, an insurance company may request the customer to provide a shareholder register or other documents to support the identification of such person(s).
2. If no natural person is identified under subparagraph VI.(i)1. or there is doubt as to whether the person(s) with the controlling ownership interest is the beneficial owner(s), the insurance company should identify the natural person(s) 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).
3. If no natural person is identified under subparagraph VI.(i)1. or VI.(i)1. above, an insurance company should identify the persons

holding the position of senior management.

(ii) For a customer that is a trustee of a trust: an insurance company should identify the settlor, the trustee, the protector, the beneficiaries, and any other natural person exercising ultimate effective control over the trust, or the persons in equivalent or similar positions.

(iii) The requirements under subparagraph III(iii) do not apply to a customer or a person having control over the customer that is one of the following entities, unless the customer or the person meets the description provided in subparagraph III(i) or subparagraph III(ii) or has issued bearer shares:

1. R.O.C government;
2. R.O.C. government-owned enterprise;
3. Foreign government;
4. Domestic public company or its subsidiaries;
5. Company listed in other jurisdiction where it is required to disclose majority shareholders, and the subsidiaries of such company;
6. Financial institution supervised by R.O.C. government, and investment vehicle managed by such financial institution;
7. Financial institution incorporated or established in other jurisdiction where it is subject to regulatory requirements that are consistent with FATF AML/CFT standard, and investment vehicle managed by such financial institution. An insurance company should retain relevant documentation (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.) with respect to such financial institution and investment vehicle.
8. Certain funds managed by R.O.C. government; or
9. Employee stock ownership trust, or employee savings ownership trust.

(iv) When the clients apply for property insurance, casualty insurance, health insurance, or insurance products not having of the policy reserves value, the provisions in subparagraph 3 do not apply to identify and verify the real beneficiary unless the clients come from high-risk countries or regions where have not adopted effective control of money-laundering

or the financing terrorism and so being suspicious of the clients or transactions for money-laundering or the financing terrorism.

VII. For a customer with whom an insurance company establishes business relationship, the insurance company should take following measures to verify the identity of the customer, the person acting on behalf of the customer, and the beneficiaries of the customers:

(i) Verification through documents:

1. Individual:

(1) 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 may not obtain original copies of the aforementioned document for verification, or 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 beneficiaries. 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.

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

2. Entity or trustee of a trust: 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 jurisdiction where the financial institution is located is one of jurisdictions described in subparagraph III of paragraph 1 of Article 6.

(ii) Verification through non-documentary methods (if necessary), for example:

1. Contacting the customer by telephone or letter after establishing business relationship.
2. Checking references provided by other financial institutions.
3. Cross-checking information provided by the customer with other reliable public information or private database, etc.

VIII. For a customer identified by an insurance company as a high-risk customer or a customer that has certain high-risk factors in accordance with the insurance company's relevant requirements on customer ML/TF risk assessment, the insurance company should perform enhanced verification, for example:

(i) 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.

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

(iii) Site visit.

(iv) Obtaining prior insurance company reference and contacting with the insurance company regarding the customer.

IX. An insurance company is not allowed to establish business relationship with a customer before completing CDD. If following requirements are met, however, an insurance company may complete verification after the establishment of the business relationship following the obtaining of identification data of the customer and beneficiaries:

(i) The ML/TF risks are effectively managed. This includes the insurance company should take risk control measures with respect to the scenario that a customer may take advantage of verifying identity after transaction completed;

(ii) This is essential not to interrupt the normal conduct of business with customers; and

(iii) The insurance company ensures verification of the identity of the customer and beneficial owner is carried out as soon as it is reasonably practicable. If the insurance company fails to complete the verification of identity of the customer and beneficiary in a reasonably practicable

timeframe, it should terminate the business relationship with the customer and inform the customer in advance..

X. 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:

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

(ii) 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.

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

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

1. There is no suspicion of ML/TF;
2. The customer is assessed as a low ML/TF risk customer;
3. The transaction is approved by senior management, whose level is determined on the basis of the insurance company's internal consideration for risk; and
4. The names of recipients do not match with lists established for AML/CFT purposes.

(v) If there is any doubt as to the authenticity, appropriateness or intention of the customer or beneficial owner, the exception provided in subparagraph XI.(iv) does not apply.

(vi) A insurance company should determine the "reasonably practicable timeframe" provided in subparagraph X.(iii) based on a risk-based approach to the extent that timeframes are differentiated according to risk level. For example:

1. The insurance company should complete customer identity verification no later than 30 working days after the establishment of business relationship.
2. If customer identity verification remains uncompleted 30 days after the establishment of business relationship, the 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).

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

XI. 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 beneficiaries:

(i) 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.

(ii) 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.

XII. When conducting CDD, an insurance company should utilize an in-house database or external source information to determine whether the customer, its beneficiaries or persons holding senior management position in the customer are or were politically exposed persons ("PEPs") entrusted by a domestic or foreign government or international organization.

(i) If the customer and its beneficial owners are PEPs entrusted by a foreign government, the insurance company should treat such customer as a high-risk customer and take enhanced due diligence ("EDD") measures provided in subparagraph (i) of paragraph I of Article 6.

(ii) If the customer and its beneficiaries are PEPs entrusted by a domestic government or international organization, the insurance company should perform risk assessment when establishing business relationship with the customer and re-perform in every subsequent year. For a customer treated by the insurance company as a high-risk customer, the insurance

company should take EDD measures provided in subparagraph (i) of paragraph I of Article 6.

(iii) If the persons holding senior management position in the customer are PEPs entrusted by a domestic or foreign government or international organization, the insurance company should take into account the influence that such person exerts on the customer, to determine whether the customer is subject to EDD measures provided in subparagraph (i) of paragraph I of Article 6.

(iv) For PEPs that had been entrusted by a domestic or foreign government or international organization, the insurance company should take into account relevant risk factors to assess their influence, and determine whether they are subject to the requirements under (i) to (iii) above by applying a risk-based approach.

(v) The requirements under (i) to (iv) above also apply to family members and close associates of PEPs. The scope of aforementioned family members and close associates should be determined in accordance with the regulations established under paragraph 4 of Article 7 of Money Laundering Control Act.

(vi) The requirements under (i) to (v) do not apply to the beneficiaries of or persons holding senior management positions in the entities described in subparagraph (iii) 1 to 3 and 8.

XIII. Other requirements that an insurance company should comply with when conducting CDD:

(i) Due diligence exerted in underwriting

1. Regarding insurance applications by individuals, sale persons should request applicants/assureds to provide identity certificates(ID cards, passports, driver's license or other certificates proven their identity etc.)or make record of them.
2. Regarding insurance applications by legal persons, they are requested to provide qualified certificates of registration of the lawful certification of agents (such as business license and other licenses or registration).
3. When conducting CDD, if necessary, secondary identity certificates other than ID cards and registry certificates are

requested to provide with. Those secondary ones should be identifiable. Inventory of institution and school establishments, if can prove identity, could be treated as secondary ones. If the parties refuse to provide, and the insurance company should politely decline or wait until after verifying the identity truly.

4. Regarding insurance applications by agents of clients , follow in accordance to subparagraph 2 of paragraph 3 of this article.

(ii) CDD procedures after completion of underwriting

1. Refunds of withdrawal of insurance contracts of huge premiums (the definition of huge set by each company)are requested, motives and identify of clients should be verified to prevent money laundering or financing terrorism by means of insurance.
3. Regarding applications by agents of clients for amendments on insurance contracts, conform to provisions in accordance to subparagraph 2 of paragraph 3 of this article.

(iii) directions in exerting due diligence when insurance amount being paid.

1. When the insurance payment flows are suspicious, the insurance company should check out and investigate. If clients request to cancel a check prohibited endorsement, their motives should be understood, and appropriate notes are made.
2. verify if the processes/procedures of change in beneficiaries are normal and reasonable.
3. Verify the payees of insurance payment to check out if the amount of payment conform to their occupation of status normally and reasonably.
4. Regarding insurance claims by agents on behalf of clients , follow provisions in accordance to subparagraph 2 of paragraph 3 of this article.

(iv) For a non-face-to-face customer, the 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.

(v) For a customer establishing business relationship with the insurance company through internet, the insurance company

should comply with relevant operating Model Guidelines developed by the insurance companies

(vi) For a customer that fails to complete relevant CDD procedures, the insurance company should consider reporting a suspicious ML/FT transaction regarding to the customer.

(vii) When the insurance company suspects certain customers or transactions may be involved in ML/FT and reasonably believe that performing CDD procedures may allow the customer aware of such information, the insurance company may not implement such procedures and instead report a suspicious ML/TF transaction.

XIV. In the case that a customer in a business relationship or transaction is described in subparagraph I.(viii), an insurance company should report suspicious ML/TF transaction in accordance with Article 10 of Money Laundering Control Act. If such customer is a designated individual or entity sanctioned under Counter-Terrorism Financing Act, the insurance company is prohibited from the activities described in paragraph 1 of Article 7 of Counter-Terrorism Financing Act since the date of knowledge, and should report in accordance with the requirements of Counter-Terrorism Financing Act (please download the reporting format on the website of the Investigation Bureau, Ministry of Justice). If the insurance company is involved in the activities described in the subparagraph 3 and 4 of paragraph 1 of Article 6 of Counter-Terrorism Financing Act before aforementioned individuals or entities are listed as designated individuals or entities, the insurance company should obtain the approval of Counter-Terrorism Financing Committee in accordance with relevant regulations established under Counter-Terrorism Financing Act.

Article 5

The CDD measures conducted by an insurance company should include following requirements in ongoing due diligence on customer identity:

I. The insurance company examines identity of existing customer ,according to importance and risk levels, and take into account the date conducted CDD measures and sufficient data obtained ,and should review in appropriate time existing relationship. The appropriate timing at least include one of the followings：

i. Abnormal increase in sum-insured by a client or increase in new

transactions

ii. Periodical review timing according to the importance and risks level

iii. Major changes in status and background information of clients

II. The insurance company should scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the insurance company's knowledge of the customer, their business and risk profile, including where necessary, the source of funds.

III. The insurance company should periodically review the adequacy of the information used to identify customer and beneficial owners and ensure the update of such information. High-risk customers, especially, should be subject to at least annual review. For other customers, the insurance company should determine the frequency of review by applying a risk-based approach.

IV. When conducting CDD measures, an insurance company may rely on the customer identification data previously obtained and kept, and is not required to conduct such measures each time when the customer processes a transaction. If the insurance company has doubts about the veracity and adequacy of previously obtained customer identification data, identifies a suspicious ML/TF transaction, or there is material change in the transaction or account activities of the customer that is inconsistent with its business profile, the insurance company should re-conduct CDD measures in accordance with the requirements of Article 4.

Article 6

An insurance company should determine the extent to which it conducts CDD and ongoing due diligence measures described in paragraph 3 of Article 4 and Article 5 by applying a risk-based approach, including:

I. For higher risk situations, the insurance company should take enhanced CDD and ongoing due diligence measures, which at least include following additional enhanced measures:

(i) Before establishing or adding new business relationship, the insurance company should obtain the approval of certain level senior management, determined according to the insurance company's internal consideration of risk.

(ii) The insurance company should take reasonable measures to understand the source of wealth and source of funds of the customer. The source of funds refer to the original source that generates such funds (e.g. salary,

investment proceeds, disposal of real estate, etc.)

(iii) Conducting enhanced ongoing monitoring of the business relationship.

II. For customers from high ML/TF risk jurisdictions, the insurance company should apply enhanced measures proportionate to the risks.

III. For lower risk situations, the insurance company may take simplified measures commensurate with the lower risk factors. Simplified measures, however, should not be permitted in one of the following situations:

(i) Customers are high ML/TF risk jurisdictions, which include but are not limited to the jurisdictions, published by international anti-money laundering organizations and notified by FSC, that have serious deficiencies in AML/CFT, and other jurisdictions that fail to comply with or completely comply with the recommendations of such organizations.

(ii) The insurance company has sufficient reason to suspect the customers or transactions may be involved in ML/TF.

An insurance company may take following simplified due-diligence measures:

I. Lower the frequency of updating customer identification data.

II. Lower the extent to which the insurance company conducts ongoing monitoring, and review transactions that reach a reasonable amount.

III. The insurance company is not required to collect specific information or take special measures to understand the purpose and the nature of the business relationship if these can be inferred from the transaction types or existing 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 when CDD measures have previously been undertaken and the adequacy and sufficiency of data obtained.

Article 7

An insurance company should perform CDD measures by itself. If regulatory requirements or FSC otherwise permits the insurance company may reply on third-

parties to identify and verify the identity of customers, the person on behalf of the customer, or beneficial owners of the customer, or the purpose or nature of business relationship, the ultimate responsibility for CDD measures remain with the insurance company relying on the third party, which should be required to:

I. Obtain immediately the necessary information concerning CDD measures.

II. Take measures to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay.

III. Satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements.

IV. Satisfy itself that the jurisdiction where the third party is located has AML/CFT regulatory requirements consistent with FATF standard.

Article 8

An insurance company's mechanism for name screening on customers and related parties of a transaction should be conducted as follows:

I. The insurance company should establish policies and procedures for name screening on customers and related parties of a transaction, by applying a risk-based approach, to detect, match, and filter whether customers, persons holding senior management position of a customer, beneficial owners of a customer, or related parties of a transaction are designated individuals or entities sanctioned under Counter-Terrorism Financing Act, or terrorists or terrorist groups identified or investigated by foreign governments or international organizations. In the case of true hit, the insurance company should undertake the measures provided in subparagraph XVI of Article 4.

II. The policies and procedures for name screening on customers and related parties of a transaction should include at least the logic of matching and filtering, the operating procedure for name screening, and the standard of review, and should be documented.

III. The insurance company should record the result of name screening, and keep such record in accordance with the requirements of Article 13.

IV. The name screening mechanism should be subject to testing, including:

(i) Whether the sanction list and threshold setting are determined by

applying a risk-based approach.

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

(iii) The logic of matching and filtering.

(iv) Model validation.

(v) Whether data output is correct and complete.

V. The 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's ongoing monitoring of accounts and transactions should be conducted as follows:

I. The insurance company should integrate customer information data and transaction data throughout the company step-by-step by information systems for enquiries processed by the head office or branch for the purpose of AML/CFT, in order to enhance its capacity of account and transaction monitoring. With respect to the customer data requested or enquired by each business unit, the insurance company should establish an internal control procedure and ensure the confidentiality of the data.

II. The insurance company should establish policies and procedures for ongoing monitoring of accounts and transactions by applying a risk-based approach and use information systems to assist the identification of suspicious ML/TF transactions.

III. The insurance company should review its policies and procedures for ongoing monitoring of accounts and transactions and update periodically to take into account regulatory requirements on AML/CFT, customer profiles, the size and complexity of business, the trend and information related to ML/TF obtained from internal or external sources, the result of internal risk assessment, etc.

IV. Policies and procedures for ongoing monitoring of accounts and transactions should include at least complete and documented monitoring types, parameters, thresholds, operating procedures for the conducting and monitoring of alerts, procedures for reviewing monitoring cases, and the standard of reporting.

V. The mechanism provided in last subparagraph should be subject to testing,

including:

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

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

(iii) The logic of detection scenario.

(iv) Model validation.

(v) Data input.

VI. In the cases where the 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 ML/TF, regardless of the amount, value, or whether transactions are completed, the insurance company should perform enhanced review of the customer identity.

VII. The red flags for suspicious ML/TF transactions provided in the Annex are not exhaustive. The 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 ML/TF risk assessment or information of daily transactions, to identify red flag transactions of potential ML/TF.

VIII. For red flag transactions identified in accordance with last subparagraph, the 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, unrelated to the customer's business profile, do not match the customer's business model, no reasonable economic purpose, no reasonable explanation, no reasonable purpose, or unclear source of funds or explanation) and keep review records. If the insurance company determines such transaction is not a suspicious ML/TF transaction, the insurance company should record the reason for the decision. If the insurance company determines such transaction is suspicious ML/TF 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 ML/TF transaction.

IX. With respect to red flags for suspicious ML/TF transactions, the 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, the insurance company should also, by other means, assist employees to determine whether transactions are suspicious ML/TF transactions when they are processed by customers. The assistance of information system cannot replace the judgment of employees. The insurance company is still required to strengthen employee training to allow employees capable of identifying suspicious ML/TF transactions.

Reporting of suspicious ML/TF transactions:

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

II. 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 immediate request the employee complete a report (please download the reporting format on the website of the Investigation of Bureau, Ministry of Justice).

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

IV. After the report is submitted by the responsible unit and approved by AML/CFT Responsible Officer, the insurance company should file the report, within 10 working days from the date of suspicious M/L transactions uncovered, to the Investigation of Bureau, Ministry of Justice.

V. In the case of an apparently significant and urgent suspicious ML/TF transaction, the 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. The 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, the insurance company should retain the fax reply.

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

I. Employee at all levels should keep the reporting of suspicious ML/TF 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.

II. 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.

III. AML responsible unit, compliance officers or internal auditors should be able to timely obtain customer identification data and transaction record to the extent that requirements on confidentiality are met.

An insurance company should record the result of monitoring of accounts or transactions and keep such record in accordance with the requirements of Article 13.

Article 10

Prior to the launch of new products or new business practices (including new payment mechanism, the use of new technologies for pre-existing or new products or businesses), an insurance company should perform ML/TF risk assessment for such products or business practices and take measures to manage and mitigate the risks identified.

Article 11

An insurance company should comply with following requirements on currency transactions above a certain amount:

I. The insurance company should verify customer identity and retain relevant documentation.

II. The insurance company should comply with following requirements on the measures of the verification of customer identity:

(i) 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, the insurance company may not

verify the identity but describe the transaction is processed by the account owner on transaction records.

(ii) In case where the transaction is processed by a person acting on behalf of the customer, the 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.

(iii) In case where the transaction is an occasional transaction, the insurance company should verify the customer identity in accordance with the requirements of subparagraph III of Article 4.

III. Except for the situations described in paragraph 2 and paragraph 3, the 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 the insurance company fails to complete media reporting with a justified reason, it may submit a hard copy of the report after obtaining the approval from the Investigation of Bureau, Ministry of Justice.

IV. The insurance company should retain the reporting data and relevant documentations submitted to the Investigation of Bureau, Ministry of Justice in accordance with the requirements of Article 14.

The insurance company is exempt from reporting following currency transactions above a certain amount to the Investigation of Bureau, Ministry of Justice but remains required to verify customer identity and retain relevant documentations:

I. 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.

II. Payments collected or maid for a government treasury by a financial institution acting as its commissioned insurance company.

III. Payment collected under a collection service (excluding the payments deposited into an account used to collect capital contribution from shareholders, and payments collected for credit card bill), provided that the payment notice clearly specifies the counterparty's name, identification number (including a reference number which permits traceability of the transaction party's identity), type and amount of the transaction. However, the duplicate copy of the payment notice should be retained as an evidence of the transaction.

For an entity account opened by department stores, wholesale stores, convenience store chains, gas stations, hospitals, clinics, transportation businesses, restaurants, and hotels, etc. which must often or regularly deposit cash above a certain amount based on business needs, the insurance company may, after verifying such needs, submit a list of such entities to the Investigation Bureau, Ministry of Justice for approval. If the Investigation Bureau, Ministry of Justice provide no comment against the list, payments deposited into such account ,within 10 days, are exempt from verification and reporting on a case-by-case basis.

The insurance company should perform at least annual review of the counterparty. If the counterparty with which the insurance company no longer has the business relationship described in this paragraph, the insurance company should report to the Investigation Bureau, Ministry of Justice.

For the transactions described in previous two paragraphs, in case where a suspicious ML/TF transaction is identified, the insurance company should remain subject to the requirements of Article 10 of Money Laundering Control Act and paragraph 2 of Article 7 of Counter-Terrorism Financing Act.

Article 12

Reporting of properties or interest of properties and location sanctioned by article 7 of AML act, in accordance with one of the following requirements：

I. Within 10 working day since the date of knowledge of objects sanctioned, the insurance company should ,approved by the AML/CFT Responsible Officer , file the report, in the reporting format/means set out by the Investigation of Bureau, Ministry of Justice, immediately to the Investigation of Bureau, Ministry of Justice.

II In the case of an apparently significant and urgent suspicious ML/TF transaction, the 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. The 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 the format set out by the Investigation of Bureau, Ministry of Justice. In addition, the insurance company should retain the fax reply.

III. An insurance company should base on Dec. 31 annually as a date closing, making annual report in the format set out by the Investigation of Bureau, Ministry of Justice, which record properties or interest of properties and location, of individuals/legal persons/groups designated to be sanctioned by article 7 of AML act. The insurance company should submit before Mar.31 the following year to the Investigation of Bureau for record reference.

Article 13

An insurance company should keep records on customers and transactions with hard copies or electronic data in accordance with following requirements:

I. The insurance company should maintain, for at least five years, all necessary records on transactions, both domestic and international. However in case where laws otherwise provide a longer period for record-keeping, the insurance company should comply with such laws. The aforementioned necessary records include:
   (i) The name, or account number or identifier of each party involved in a transaction.
   (ii) Date of transaction.
   (iii) Currency and amount of transaction.
   (iv) The way funds are deposited or withdrew, such as cash, checks, etc.
   (v) Destination of funds.

II. For currency transactions above a certain amount, the 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, the 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.

III. For the reporting of a suspicious ML/TF transactions, the bank should keep relevant records of reporting for at least 5 years in the original manner.

IV. The Insurance company should keep following information after the business relationship is ended, or after the date of occasional transaction for at least 5 years. However in case where laws otherwise provide a longer period for record-keeping, the Insurance company should comply with such laws:

(i) All records obtained through the CDD measures, e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents.

(ii) Insurance contract files.

(iii) Business correspondence, including the information of the background or purpose of complex, unusual large transactions obtained from enquiries, and the result of any analysis undertaken.

V. The records kept by the insurance company should be sufficient to permit reconstruction of individual transactions so as to provide evidence for the determination of criminal activity.

VI. The Insurance company should ensure to rapidly provide transaction records, the CDD information, and relevant information, etc. to competent authorities upon appropriate authority.

Article 14

Others that require attention:

I..An insurance company should exerting attention on and understand the motives of a client or a salesperson who is suspicious of avoiding the requirements in accordance in AML act, such as spreading the insurance amount of insurance contracts with huge sum insured by applicants/assureds among different insurers

II. Annual review of internal audit of AML/CFT is required to check if present measures are sufficient. Any noncompliance found in units of the company must be corrected in time.

III.In process of investigation on suspicious employees involved in money laundering/financing terrorism, confidentiality of such cases must be safeguarded carefully.

Article 15

Responsible unit and responsible officer:

I. The Insurance company should deploy adequate and sufficient AML/CFT officers and resources according to its size and risks, etc. The board of directors should appoint a senior officer to serve as AML/CFT responsible officer, who should be sufficiently authorized to coordinate and supervise AML/CFT affairs, and ensure such officers and responsible officer do not take other responsibility which conflicts with their AML/CFT responsibilities.

II. Responsible unit and responsible office described in last subparagraph are in charge of following affairs:

(i) Supervising the planning and implementation of policies and procedures for identifying, assessing and monitoring ML/TF risks.

(ii) Coordinating and supervising the implementation of the insurance company-wide ML/TF risk identification and assessment.

(iii) Monitoring risks related to ML/TF.

(iv) Developing AML/CFT programs.

(v) Coordinating and supervising the implementation of AML/CFT programs.

(vi) Confirming the compliance with relevant AML/CFT regulatory requirements, including relevant Model Guideliness or self-regulatory rules established by associations of financial services industry and approved by FSC.

(vii) Supervising the reporting of suspicious ML/TF transactions and properties or property interests and locations of designated individuals or entities sanctioned under Counter-Terrorism Financing Act to the Investigation Bureau, Ministry of Justice.

(viii) Other related affairs concerning AML/CFT.

III. The responsible officer described in subparagraph I 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, responsible officer should immediate report to the board of directors and supervisors (board of supervisors) or audit committee.

IV. A foreign business unit of the insurance company should deploy adequate and sufficient AML/CFT officers by taking into account the number of local branches, size of business, risks, etc. and appoint a head responsible for supervising AML/CFT affairs.

V. The appointment of AML/CFT head of the 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 responsible office described in subparagraph 1, and should not take other responsibilities except compliance head. In case where the head may take other responsibilities, the insurance company should discuss with local competent authorities to ensure such arrangement has no concern in conflict of interest and report to FSC for reference.

Article 16

The implementation, audit, and statement of the AML/CFT internal control system:

I. A domestic and foreign business unit of an insurance company should appoint a senior officer to serve as a supervisory officer responsible for supervising the implementation of AML/CFT and the implementation of self-inspection pursuant to relevant requirements of business unit.

II. The internal audit unit of an insurance company should audit and provide auditor opinion on following matters:
   (i) Whether ML/TF risk assessment and AML/CFT programs meet regulatory requirements and are implemented.
   (ii) The effectiveness of AML/CFT programs.

III. Responsibilities of internal audit unit:
   (i) Determining the matters subject to audit according to internal control measures and relevant regulations, conducting periodic audit, and testing the effectiveness of AML/CFT programs and risk management quality of operations, departments and branches (or subsidiaries).
   (ii) The auditing method should cover independent transaction testing, including selecting transactions related to high-risk products, customers, and geographic areas to verify the insurance company has effectively implemented relevant AML/CFT regulatory requirements.
   (iii) In case where any deficiency in the implementation of specific management measures is identified, internal audit unit should periodically report to AML/CFT responsible officer for review and

provide such information as a reference of employee training.

(iv) 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.

IV. An insurance company's chief executive officer should supervise each unit to the extent that the implementation of AML/CFT internal control system is assessed and reviewed by each unit in a prudent manner. The chairman, chief executive officer, chief auditor, and AML/CFT responsible officer should jointly issue a statement for AML/CFT internal control system and submit to board of directors for approval. Within 3 months after the end of each fiscal year, the insurance company should disclose the statement on its website and publish the statement through a website designated by FSC.

V. For a branch of a foreign insurance company located in Taiwan, the requirements of the Model Guidelines regarding the board of directors or supervisors may be satisfied by persons authorized by the head office. The statement described in last subparagraph may be jointly issued by a representative for litigious and non-litigious matters, AML/CFT responsible officer, and a senior auditor responsible for Taiwan area, etc.

Article 17

Employee hiring and training:

I. An insurance company should establish prudent and appropriate procedures for screening and hiring employees, including reviewing whether a candidate has decent personality and professional knowledge required for the job.

II. An insurance company's AML/CFT responsible officer, AML/CFT officers, and domestic business unit supervisory officers should meet one of following requirements within 3 months after the appointment. The insurance company should establish relevant control mechanism to ensure the compliance of such requirements:

(i) Having at least 3-year experience as a compliance officer or AML/CFT officer.

(ii) Attending at least 24-hour training classes provided by an institution recognized by FSC and obtaining a certificate of completion after

passing an exam. For a person who has been qualified for a compliance officer, however, may be treated as meeting the qualification requirement provided in subparagraph II.(ii) after attending 12-hour AML/CFT training classes.

(iii) Obtaining a domestic or international AML/CFT professional certificate issued by an institution recognized by FSC.

III. In case where the officers described in last subparagraph were appointed before Aug. 31, 2017, they may be treated as meeting the qualification requirements if one of following requirements are met:

(i) Meeting the qualification requirements of subparagraph II.(i) or (ii) before Aug. 31, 2017.

(ii) Meeting the qualification requirements of subparagraph II.(ii) by one of the following deadlines:

1. For the insurance company's AML/CFT responsible officer and AML/CFT officers, within 6 months after the appointment.
2. For the insurance company's domestic business unit supervisory officers, within 1 year after the appointment.

IV. The insurance company's AML/CFT responsible officer, AML/CFT officers, and domestic business unit supervisory officers should attend at least 12-hour AML/CFT trainings each year provided by the insurance company or external training institutions agreed by AML/CFT officer described in subparagraph 1 of Article 15. Such trainings should at least cover new updates on regulatory requirements, and ML/TF trends and red flags. Those who obtain domestic or international AML/CFT professional certificates issued by an institution recognized by FSC may be exempt from satisfying the requirements on training hour for the same year.

V. The insurance company's foreign business unit supervisory officer and AML/CFT head and officers should have AML expertise, be familiar with local regulatory requirements, and attend 12-hour AML/CFT trainings provided by local competent authorities or relevant institutions. In case where local competent authorities or relevant institutions do not provide AML/CFT trainings, such persons may attend the trainings provided by the insurance company or external training institutions agreed by AML/CFT responsible officer described in subparagraph 1 of Article 15.

VI. The insurance company should arrange AML/CFT trainings each year that have appropriate contents and training hours determined according to the nature of business for its directors, supervisors, chief executive officer, compliance officers, internal auditors and salesmen, to allow them to understand their AML/CFT duties and have the expertise required for such duties

VII. An insurance company may take following measures to conduct relevant trainings for all employees to learn, in order to strengthen the judgment of employees, implement AML/CFT functions, and prevent employees from non-compliance. Such trainings may invite scholars or experts from ministry of justice or FSC /university /other institutions as instructors if necessary.

In job trainings/study abroad, employees should take advantage of opportunities to learn practical measures in AML/CFT taken by foreign insurance companies. If any measure works, an insurance company should reward the employee.

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. Attempting to persuade employees not to collect data that is required to complete the transaction.
3. Enquiring the possibility of avoiding being reported.
4. Eager to explain the source of fund is clean or the transaction is not for money laundering purpose.
5. 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 Guidelines for Non-life Insurance Enterprise's Anti-Money Laundering and Countering Terrorism Financing ("Guidelines") by reference to the Model Guidelines and implement the Guidelines 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 NLIA and report to the FSC for recordation after the implementation.