Guidance for Insurance Sector on the Best Practices for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Compliance

Foreword:
The best practices guidance is provided for the reference of insurance companies in undertaking anti-money laundering and combating the financing of terrorism (AML/CFT) operation. It is not meant to be mandatory. An insurance company may, based on the nature and size of its business and in consideration of the results of risk assessment in the areas of geographic locations, customers, products and services, transactions and delivery channels, select the most appropriate best practices to prevent or reduce money laundering and terrorist financing (ML/TF) risks.

Identification and verification of a legal person's beneficial owner(s)

I. Threat and weakness analysis

（Ⅰ） Source of threat and analysis

Advancement and information technology and changes in the international trade environment have contributed to newer and more advanced criminal offenses through organized operations. Among these offenses include money laundering, tax evasion, massive transfer, and concealment of funds through the use of legal persons or associations which have attracted the attention of the international society. To prevent such occurrences, understanding and confirming the beneficial owners of legal persons or associations have become the most urgent tasks.

Public companies are applicable to the Securities and Exchange Act and they are obligated to announce and report various general and material information. In addition, such companies

are also required to upload and disclose their financial reports or annual reports that have been audited by their CPAs and they thus exhibit a certain degree of information transparency. Therefore, the Regulations Governing Anti-Money Laundering of Financial Institutions expressly provides that the identification and verification of the beneficial owners may be exempted for customers who are publicly-listed companies in the R.O.C. or their subsidiaries. However, the identification and verification of beneficial owners of non-public companies, other civil associations and groups, or foreign corporate shareholders for determining the natural persons with actual controlling rights over legal persons or groups pose the highest threats to transactions with legal persons and group customers.

（II）Weakness analysis

The biggest challenge in the identity verification of legal person or group customers is “information opacity” and the “information asymmetry” with financial institutions. Information on the actual owners and individuals with actual controlling rights of legal persons or groups, regardless of whether they obtain such rights through shares held, capital contribution, actual control over personnel or decisions, or service as senior managers, are internal information of the legal persons or groups. Such “internal information” pose a certain degree of information opacity and information cannot be easily reviewed or verified by financial institutions. It therefore contributes to the “information asymmetry” that prevents comprehensive and effective KYC and identification of beneficial owners.

As a result of the aforementioned weaknesses derived from “information asymmetry”, financial institutions have often relied excessively on customers’ statements. In reality, the veracity of

statements cannot be positively determined even if statements are signed by the authorized signatories of legal persons or groups. Therefore, according to Article 3, Subparagraph 7 of the Regulations Governing Anti-Money Laundering of Financial Institutions, insurance companies shall use the following information to identify the beneficial owner(s) of the customer and take reasonable measures to authenticate the identity of such persons. In addition, Article 4, Subparagraph 8, Item 1 of the Model Guidelines Governing Anti-Money Laundering and Countering Terrorism Financing of Life Insurance Companies also stipulates: "Life insurance companies may, in accordance with its own operational procedures, ask the legal person, group, or representative thereof, to issue a statement regarding the information of the beneficial owners, but it is required that at least a portion of the information specified in the statement be verifiable by other reliable documents or sources of information such as documents evidencing company registration or company annual reports."

Therefore, even if the customer's statement is adopted as the method for verifying the identity of the beneficial owners, insurance companies may not rely excessively on the unilateral statements of the customer and they must adopt necessary verification measures for the statements and the contents therein to verify the identity of the beneficial owners. However, the verification of customers' statements and the identity of the beneficial owners may differ due to the customer type (companies, associations, foundations, and various non-legal person associations such as partnerships, temples, cram schools, firms, trade (union) associations, management committees, etc.). They may lack official or public information which can be used as the basis for information verification. Therefore, a set of

consistent and effective practical practices has not yet been formed. Therefore, financial institutions are actually excessively reliant upon customers' statements when faced with the threat of "information asymmetry" and they lack effective verification platforms and methods. There are undeniable weaknesses exhibited in the difficulty for verifying the veracity of statements regarding beneficial owners.

II. Practical references

（Ⅰ） Related rules regarding procedures for identifying beneficial owners have been established in the Template of Directions Governing Anti-Money Laundering and Combating the Financing of Terrorism.

（ⅠⅠ） As for non-natural persons, it is advisable to obtain their establishment and registration certification documents, company change registration table, and other documents sufficient for identity verification. In addition, individual certification documents shall be obtained in accordance with the organization type. For instance, registration/establishment/permit licenses, company change registration table, or other registration/establishment, business/operation approval form issued by competent authorities shall be required for companies limited by shares, limited companies, small and medium enterprises. After obtaining the certification documents, financial institutions shall verify their veracity based on public information such as the Market Observation Post System, company and business registration inquiries on the MOEA website, for-profit business inquiries on the website of the Ministry of Finance, civil association registration inquiries on the website of the Ministry of the Interior, or other information inquiry services announced by other competent authorities (e.g. Bureau of Education of local governments). It is advisable to

print the search results of public information and save them for future reference.

（III） Target and timing of identification:

1. Proposer: The proposer is a party to the insurance contract. As the proposer is a customer of the insurance company, it is advisable to request the proposer fill out the “Beneficial Owner(s) Identification Statement” when filling out the insurance application documents.
2. Beneficiary: Although the beneficiary is not a party to the insurance contract, it is the ultimate recipient of the insurance payment and the ultimate beneficiary. If the beneficiary is not a natural person, the identification of its beneficial owner(s) shall still be required. However, if the beneficiary is requested to fill out the “Beneficial Owner(s) Identification Statement” when it applies for insurance payment and the beneficiary refuses to cooperate, it remains difficult for the insurance company to directly refuse to perform its obligations for insurance payment. Therefore, it is advisable to request the beneficiary to fill out the “Beneficial Owner(s) Identification Statement” when designating a non-natural person as the beneficiary or changing a specific non-natural person as the beneficiary. When the beneficiary applies for insurance payment, the insurance company may request a statement based on actual conditions to verify whether there are changes in the beneficial owner(s).

（IV）The following procedures are recommended for the verification of the identity of beneficial owners of proposers or beneficiaries who are not natural persons:

1. Identify shareholders who hold more than 10% of shares in corporate customers in accordance with Article 22-1 of the Company Act.

2. Principles: Submit the “Beneficial Owner(s) Identification Statement”

(1) Verify natural-person customers who directly or indirectly hold more than 25% of the company’s shares and request them to provide photocopies of shareholder registers or other shareholding certification documents and the companies’ articles of incorporation to verify the veracity of the statement filled out by corporate customers regarding shareholders with more than 25% of shares and whether issuance of bearer shares is permitted.

(2) If the customer states that it has no natural-person shareholders who hold more than 25% of direct or indirect shares, it is advisable to request the customer to fill out the individuals with actual controlling interest in the legal person (e.g. president, chief executive officer, and chief operating officer are considered as individuals with actual controlling interest). If there are no other methods to exercise controlling interest in the customer, it is advisable to verify the identity of senior executives (e.g. chairman, general manager, chief financial officer are considered as the senior executives). If the veracity of the identity of the beneficial owner cannot be verified through public information, it is advisable to request the proposer to provide photocopies of such beneficial owners or other identity verification information.

(3) If the customer is a legal person or an association that is a non-company organization which has no shareholder or capital contributor, it is advisable to directly request the customer to fill out information on the identity of the individual with controlling interest or the senior executive as its beneficial owner.

(4) It is advisable to include the name, date of birth, nationality, and number of identification documents (e.g. national ID card or passport number) in the scope of identity information of beneficial owners for comparison in the name verification system.

(5) The "Beneficial Owner(s) Identification Statement" shall be signed by the customer, related business personnel, and the supervisor who shall be held accountable for the contents.

3. Example: Government authorities, public companies, state-owned enterprises, and financial institutions are may be exempted from filling out the "Beneficial Owner(s) Identification Statement" but it is advisable to request a statement and fill out the basic information. For special conditions (e.g. entities from high-risk countries or those that have issued bearer shares), it is advisable to fill out the "Beneficial Owner(s) Identification Statement".

4. In addition to using the shareholding structure for the identification of beneficial owners, the following methods are also recommended:

(1) The legal person financial information, credit information, and other related documents can be used to obtain information on individuals with high levels of dependency in economic interests with the company and those with actual controlling interest in the company (e.g. individuals who serve as joint guarantors or provide collateral, or individuals with high levels of fund transactions with the company or specific shareholders as disclosed in financial reports).

(2) Public information on the Internet can also be used to obtain information on the legal person or association

customer to learn whether there are individuals with high levels of dependency in economic interests with the company and those with actual controlling interest in the company.

（Ⅴ） Measures for verifying beneficial owners:

1. Information on corporate customers' directors, supervisors, managerial officers, and shareholders who hold more than 10% of issued shares or total capital in corporate customers obtained from the information platform specified in Article 22-1 of the Company Act can be used as reference for verifying the identity of beneficial owners.
2. Insurance companies may obtain information on legal persons in Taiwan from the MOEA Commercial Industrial Services Portal and they may use the registered shares held by directors and supervisors to facilitate a preliminary verification of whether there are natural-person shareholders who hold more than 25% of shares.
3. They may also request shareholder registers and verify whether the shareholding structure and shareholding ratios are valid and accurate.
4. If the customer is a company listed on TWSE, OTC, emerging stocks, or a public company, it is advisable to inquire on the Market Observation Post System to verify the veracity of the information.
5. If the customer is a company listed in a foreign country or its subsidiary, it is advisable to request the full name of the issuing company and the stock exchange code and inquire the listing information of the company at the foreign exchange house.
6. In addition to filling out the "Beneficial Owner(s) Identification Statement", if the beneficial owner, individual

with controlling interest, or senior executive cannot be verified through company registration and certification documents, company change registration table, financial reports, annual reports, registered information inquiries provided the MOEA or competent authorities, or other credible documents or source of data, insurance companies are advised to obtain at least the photocopies of the identity documents.

7. Where the beneficial owners cannot be verified through the aforementioned method or where the information provided by the customer is in doubt (e.g. the information provided by the customer is inconsistent with public information and the customer cannot provide a reasonable explanation), it is advisable to decline the insurance application.

(Ⅵ) Verification of the identity of legal representatives of underage proposers or insured individuals

If the proposer or insured natural person is an underage individual and the insurance policy is signed by the legal representative, the insurance company shall regard the legal representative as the individual with actual control over the value of the policy and the policy owner. Where such conditions apply, the legal representative field in the insurance application form shall require the personal signature of the legal representative and it is also advisable to fill out information such as the legal representative's name, nationality, date of birth, or identity document number for comparison in the name screening system. It is also advisable to fill out the legal representative's name, nationality, date of birth, or identity document number in the solicitor's report.

(Ⅶ) Beneficial owner information changes and updates

Within one year of the completion of the aforementioned identity

verification for the beneficial owner of a non-natural-person proposer by the insurance company, if the proposer purchases other insurance products from the same company, it is advisable to request the proposer to verify whether there are changes to the identity information of the beneficial owner. If there are no changes, it is advisable to obtain a statement stating that there are no changes to the beneficial owner; if there are changes, it is advisable to request the proposer to fill out the "Beneficial Owner(s) Identification Statement" and execute the aforementioned verification procedures in accordance with the filled-out content.

（Ⅷ）Effects of name screening after identity verification

The beneficial owners of non-natural persons and legal representatives of natural persons shall be identified and verified through the name screening system. Where the beneficial owner is an individual designated for sanctions in accordance with the Counter-Terrorism Financing Act, the insurance company shall decline the insurance application. Where the beneficial owner is a confirmed domestic or foreign PEP, an individual involved in adverse news, or an individual on law enforcement lists, necessary enhanced review shall be implemented in accordance with the risk assessment results.

Money Laundering and Terrorist Financing Risk Management of OIU Businesses

I. Weakness analysis of OIU

（Ⅰ） State of business

Insurance companies began operating OIU businesses based on the approval of the FSC in June 2015. OIU is a relatively young

business compared to other traditional insurance businesses. As the proposer and insured for purchase of OIU insurance products must be foreign nationals, they have been restricted by the sources of customers and the scale of operations has remained small. According to the National Money Laundering and Terrorist Financing Risk Assessment Report, revenue from OIU premiums account for an insignificant proportion of overall revenue from insurance policies. Compared to the number of domestic customers, foreign customer account for only a very small portion of total customers.

（ＩＩ）Identification of threats and weaknesses

OIU transactions are insurance businesses conducted in foreign currencies and targeted at foreign nationals (including foreign individuals, legal persons, government authorities, or financial institutions outside the borders of the Republic of China). Transactions involve cross-border services and the verification of the veracity of related identity documents may be difficult or may incur high costs. Taiwan is a country with high levels of economic and trade development and its geographical location is near countries with frequent criminal activities or higher ML/TF risks. Criminal threats faced by these countries differ from those in simple domestic transactions. Insurance companies are therefore advised to learn about the possible threats of related transaction counterparties and the threats of main criminal activities in their respective countries (e.g. reference related analyses of companies in databases and the National Money Laundering and Terrorist Financing Risk Assessment Reports published by related countries).

As the current customer group policy for the OIU business does not restrict foreign PEPs or high-net-worth individuals from purchasing insurance policies and current OIU products are

denominated in foreign currencies and have high insurance policy preparatory funds, they are more likely to be used as money laundering tools by individuals connected with criminal proceeds. In addition, as it is more difficult to verify the veracity of identity verification documents provided by foreign nationals and customers may conduct transactions through insurance brokers and agencies, insurance companies often cannot directly communicate with customers and it is the main weakness in the OIU business. The criminal pattern reports, threat risk assessment reports, and statistics distributed by the Criminal Investigation Bureau of the National Police Agency, Ministry of the Interior, Investigation Bureau of the Ministry of Justice, and other law enforcement authorities can be used as references for strengthening insurance companies' knowledge of suspicious transactions patterns in criminal activities conducted by criminals in predicate offenses. The knowledge of related domestic and foreign criminal activities and the experience in investigations by law enforcement authorities shall be used to improve knowledge of behavior patterns in predicate offenses and how insurance products are used for money laundering.

Insurance companies are advised to conduct an overall assessment of the OIU business compared to the overall insurance business status (e.g. customer ratio and revenue from insurance premiums), threats faced by the OIU (e.g. cross-border services), and weaknesses in OIU businesses (e.g. difficulties in identity verification). Insurance companies shall adopt a risk-based approach and consider the impact of OIU business on the overall ML/TF risks of the entire company to identify and assess OIU risks and threats and manage and mitigate identified risks. As the recipients of OIU services are offshore customers and business products are denominated in foreign currencies, they

face different ML/TF risks compared to other traditional insurance businesses.

Insurance companies are advised to use the following threat identification and assessment in the OIU business in accordance with the results in the National Money Laundering and Terrorist Financing Risk Assessment Report. They shall also strengthen the connection of OIU businesses and the companies' overall risk indicators:

1. Customer risks: OIU service recipients are foreign nationals or foreign legal persons and they may also be foreign PEPs or high-net-worth individuals. Due to the freedom of transactions and difficulties in obtaining information or identification of foreign nationals, the verification of customers' information incur higher costs and they thus incur higher risks of abuse as money laundering channels. Companies may consider their product development and customer group acceptance policies to distinguish the risks in the customer sources based on a weight system.
2. Geographical risks: OIU service recipients are foreign nationals or foreign legal persons and they may originate from countries across the world including high-risk countries, countries of concern, or tax havens.
3. Product and service risks: OIU mainly provides personal insurance products such as high-savings insurance products or investment insurance products. Insurance transactions are paid in foreign currencies. Income tax is exempted for the interest generated from investment targets in insurance payment or income from transactions in structural products and investment insurance contracts that is paid to the OIU customer. Its nature may attract offshore customers with different purposes for purchasing insurance. In addition, as

different companies have different product policies and customer group policies, they may face different risks. Insurance companies are advised to review their customer group and product distribution status (e.g. age, professions, nationalities, etc.) where necessary and update their product policies and customer group acceptance policies.

4. Transaction and channel risks: Insurance companies conduct IOU businesses face to face through personal visits by customers to their own solicitors as well as through insurance brokers or insurance agents. In addition, if an insurance company's OIU business accepts offshore transactions, it is advisable to adopt related management measures for offshore transactions.

II. Recommendations for strengthening management measures for OIU customers

OIU services are provided for offshore customers who may be foreign PEPs, high-net-worth individuals, or legal persons registered in high-risk countries, countries of concern, or tax havens. Compared to domestic insurance businesses, it is more difficult to verify the customer's profession or the ultimate beneficial owner. Insurance companies are advised to strengthen measures for documents, data, or information required for the procedures for verifying customers' identity. Enhanced due diligence shall be executed for customers identified as high-risk customers based on the risk-based approach adopted by insurance companies. Insurance companies are also advised to analyze their customer groups to understand their composition and distribution.

The products provided in OIU businesses consist mainly of those with high insurance policy preparatory funds or cash value. Income tax is exempted for the interest generated from investment targets in insurance payment or interest and income from transactions in

structural products and investment insurance contracts. Its nature may attract offshore customers with different purposes for purchasing insurance which results in higher complexity and integration with other industries. Insurance companies are advised to adopt bank remittances or fund transfers for payment to prevent break points in the money flow caused by cash transactions. Where insurance companies encounter suspected money laundering transaction patterns that trigger suspicious transaction monitoring alerts when conducting customer due diligence or executing transactions, they may communicate with law enforcement authorities where necessary and issue suspicious transaction reports or terrorist financing reports in accordance with the Money Laundering Control Act and Counter-Terrorism Financing Act.

III. Strengthened management measures for OIUs

（Ⅰ） Recommended document, data, or information that should be obtained or verified for customer identity verification:

1. Where the proposer or insured is a natural person:

(1) Name, date of birth, nationality, address, type and number of identification documents.

(2) Obtain photocopies of at least two types of identification issued by government authorities or other identification documents with photograph that can be used to determine the identity, nationality, original residence, or permanent residence of the holder.

(3) Obtain signed response letters for letters delivered to the name and address provided by the proposer or insured, conduct telephone interviews, or conduct other identity verification measures (e.g. photocopies of water, electricity, telecommunications, or bank statements or tax filing certification documents) based on the customer's risk rating.

2. Where the proposer is a legal person:

(1) Obtain the full name, registration date and location, registration number, registered address, and address of main business operations.
(2) The Certificate of Incorporation issued by the registry Institution of the place of registration.
(3) Articles of Incorporation.
(4) The Certificate of Incumbency issued by the local registration agency of the legal person's place of registration within the last 6 months.
(5) Certificate of Good Standing signed and issued by local registration agency of the legal person's registered region in the past 6 months.
(6) List of directors, shareholders, and senior management personnel.
(7) Photocopies of meeting minutes or authorization letter regarding the signing of the insurance contract submitted by the proposer unit (the content shall specify at least the name of the authorized individual and personnel included in the insurance coverage).
(8) Photocopies identification documents of the person in charge or authorized individual.
(9) Obtain signed response letters for letters delivered to the name and address provided by the proposer or insured, conduct telephone interviews, or conduct other identity verification measures (e.g. photocopies of water, electricity, telecommunications, or bank statements or tax filing certification documents) based on the customer’s risk rating.

3. If the customer is unwilling to cooperate or fails to provide identity information or documents for verification, insurance companies are advised to decline the establishment of business relations with the customer.

（II）Enhanced customer due diligence and transaction monitoring

Enhanced due diligence shall be executed for customers identified as high-risk customers based on the risk-based approach adopted by insurance companies. Insurance companies shall adopt reasonable measures to understand the sources of the customer's wealth and funds and they are advised to use the following enhanced due diligence measures for OIU customers: Use documents such as reports filled out by sales personnel, insurance application forms filled out by customers, financial disclosure statements, customer compatibility assessments to understand the customer’s purpose for entering the country, identity, motives for purchasing insurance policies, source of funding, and cross-reference and compare the background information. Evaluate information including the customer’s age, work content, company of employment, purchased insurance products, amounts, and motives for purchasing insurance in the overall assessment. Where irregularities are found in the documents provided for review, where funds are discovered to be associated with ML/TF activities, or where insurance companies encounter suspected money laundering transaction patterns that trigger suspicious transaction monitoring alerts when conducting customer due diligence or executing transactions, they may communicate with law enforcement authorities, provide information where necessary, and submit suspicious transaction reports or terrorist financing reports in accordance with the Money Laundering Control Act and Counter-Terrorism Financing Act.

（III）Renewed customer identity verification procedures for existing OIU customers

For existing customers prior with whom insurance companies have established business relations prior to August 18, 2017,

insurance companies have requested customers to provide documents, data, or information for verification before the end of 2017 and completed renewed customer identity verification procedures in accordance with regulations. However, where customers have been notified multiple times but fail to update their information, insurance companies shall adjust risk ratings based on case information and transaction status or file an STR based on the approval of the AML officer.

Practical references for strengthening and simplifying customer due diligence and continuous monitoring mechanisms for the insurance industry through the use of the risk-based approach

I. Customer transaction categorization under the risk-based approach

Insurance companies are advised to establish specific risk assessment items in accordance with the risk-based approach (it is advisable to include at least geographical, customer, product/service, transaction, and channel risk items) to assess risks in transactions and classify them into “high risk transactions”, “average risk transactions”, and “low risk transactions” for additional monitoring and control and to reduce or prevent such risks. For high-risk transactions determined by factors such as high-risk geographical location, customers, products and services, transactions, and channels, insurance companies are advised to adopt enhanced due diligence and continuous monitoring measures. For low-risk geographical location, customers, products and services, transactions, and channels, insurance companies may adopt simplified measures based on their policies, monitoring and control systems, and procedures for risk prevention.

In addition to the characteristics of their businesses, insurance

companies should also refer to the threats and weaknesses identified in the National Money Laundering and Terrorist Financing Risk Assessment Report and conduct regular/irregular reviews of the criminal pattern reports, threat risk assessment reports, and statistics distributed by the Criminal Investigation Bureau of the National Police Agency, Ministry of the Interior, Investigation Bureau of the Ministry of Justice, and other law enforcement authorities as the basis for reviewing the adequacy of customer risk classifications.

Insurance companies may consider the following high-risk factors and patterns for a comprehensive assessment of high-risk transactions:

（Ⅰ） High-risk geographical regions include countries or regions with severe AML/CFT discrepancies announced by the FATF and other countries or regions that fail to comply or comply fully with recommendations made by the FATF and forwarded by the Financial Supervisory Commission.

（ⅠⅠ）High-risk customers such as PEPs of foreign governments, terrorists or terrorist organizations under economic sanctions or designated or investigated by foreign governments or the FATF, customers whose profession involves intensive cash transaction businesses (e.g. foreign casinos, offshore companies and banks in tax/financial secrecy havens, foreign currency exchange offices, remittance brokerage companies, check exchange offices, distributors of jewelry, precious stones, and precious metals, restaurants, retailers, parking lots, etc.), non-profit organizations that are not regulated by laws, companies or trust that are susceptible to usage for holding personal assets, and customers who exhibit other high ML/TF risk patterns in business relationships.

（ⅠⅠⅠ） High-risk products and services include insurance products with high insurance premiums or high cash value, single-payment or short-period insurance products, and annuity

insurance products.

（Ⅳ）High-risk transactions and channels include OIUs and online insurance purchases.

II. Enhanced customer due diligence and continuous monitoring measures

（Ⅰ） Conditions applicable for enhanced customer due diligence and continuous monitoring

The following conditions are common high-risk transaction settings in the insurance industry and insurance companies are advised to carry out enhanced review and continuous monitoring measures:

1. Where the customer is a current PEP in a foreign government and intends to or has established a business relationship with the insurance company;
2. Where the customer is a current PEP in the domestic government or an international organization and intends to or has established a high-risk business relationship with the insurance company;
3. Where the customer is from a country or region with high ML/TF risks and intends to or has established a high-risk business relationship with the insurance company;
4. Where the customer’s cumulative insurance policy preparatory fund or account value has exceeded the threshold of high-asset customers of the insurance company by, as an example, NT$30 million;
5. Where the customer has been reported for conducting suspicious transactions by the insurance company and intends to establish a new high-risk business relationship with the insurance company;
6. Where suspected ML/TF transactions have appeared in the customer’s high-risk business relationships such as:

(1) The customer has mostly purchased insurance policies with low insurance amounts and pays insurance premiums on a regular basis but suddenly purchased large sums of single-payment insurance policies;

(2) The customer does not pay any attention to the content of the insurance or claim payments and only focuses on procedures for insurance policy loans, contract termination, or changing the beneficiary in the insurance product during the purchase;

(3) The customer uses cash to pay a large sum of insurance premiums when purchasing insurance products with high preparatory funds for the insurance value;

(4) The customer purchases insurance products with high preparatory funds for the insurance value intensively within a short period of time and the insurance policies do not appear to be commensurate with the customer's status and income or are unrelated to the nature of the customer's business;

(5) The customer deliberately evades related procedures for completing identity verification.

7. Where the customer exhibits irregular changes that are inconsistent with transactions and the nature of business in high-risk business relationships such as:

(1) An individual involved in major criminal cases reported on television, print media, or posted on the Internet attempts to purchase insurance contract products with high cash value or one who is already the proposer, insured, or beneficiary of such insurance contracts attempts to change the proposer or beneficiary or conduct transactions that involve money flow;

(2) A customer who applies for termination of contracts

intensively within a short period of time or terminates contracts with a value exceeding a certain amount and request cash payments;

(3) A customer who pays for multiple additional insurance premiums intensively within a short period of time with the sum of payments exceed a certain amount and applies for the redemption of certain parts, cancellation of contracts, termination of contracts or insurance policy loans exceeding a certain amount;

(4) A customer who apply for large sums of insurance policy loans and pays them back intensively within a short period of time and the loan amounts and repayment amounts are similar;

(5) After a change in the proposer of an insurance policy, the new proposer applies for a change of the beneficiary within a short period of time and requests a large insurance policy loan or terminates the contract;

(6) The total currency transactions of multiple cash payments and receipts (from the same account on the same business day) for the same customer exceed NT$500,000 (or the equivalent in foreign currencies);

(7) A customer who purchases a long-term life insurance policy with a large single payment and applies for a large insurance policy loan or terminates the contract within a short period of time;

(8) A customer who pays a large insurance premiums payment (including cross-border payment of insurance premiums) and applies for a large insurance policy loan or terminates the contract within a short period of time;

(9) A large insurance premiums payment that is not paid by the parties to the insurance contract or a related party;

(10) A customer with an unusually large payment or refund that is not commensurate with his/her status and income or unrelated to the nature of his/her business;

(11) A customer who uses cash or uses multiple bank accounts to pay for insurance premiums, repay insurance policy loans, or mortgages in payments that are slightly lower than the amount that requires reporting and the payments are commensurate with his/her status and income or unrelated to the nature of his/her business.

（II）Enhanced due diligence and continuous monitoring methods for high-risk customers

1. Enhanced due diligence for high-risk customers

The following items should be executed when performing enhanced due diligence on high-risk customers:

(1) Obtain additional identity verification information

a. When performing enhanced due diligence, it is advisable to consider whether additional identification information should be obtained. Examples include:

(a) Insurance application documents;

(b) Identity certification documents such as photocopies or records of passports, identity cards, driver's licenses, or similar official identity certification documents or photocopies or records of the identity certification documents of the customer or customer’s agent;

(c) Establishment documents of legal persons such as the company’s registration documents, government-issued business license, partnership agreement, trust instrument, or certification of incumbency;

(d) Information on the beneficial owners of the legal-person customer;

(e) Any name(s) or alias(es) previously used;
(f) Contact information such as telephone or mobile phone number, work address, post office box address, and email address;
(g) The nature, scope, and geographical location of the customer's profession or industry;
(h) Other information for identity verification.

b. When performing enhanced customer verification, it is advisable to consider whether additional identity verification information should be obtained. Examples include:
(a) Onsite visits or telephone call records;
(b) Past insurance transaction information;
(c) Special investigation documents such as signed records of face-to-face interviews, survival survey records, and investigation reports issued by third-parties;
(d) Reply letters which signed by the customer himself/herself or by an authorized person of the customer, legal person, or organization, and which is in reply to a letter mailed to the address provided by the customer;
(e) Background or purpose information and analysis data for complex and unusual transactions, purpose and nature of business relationships, and information on the customer's wealth and sources of funding.

c. When executing enhanced customer identification and verification measures, it is advisable to verify the additional identity verification information obtained through methods used for documents or non-documents. Examples include:

(a) Cross-verification with the identity information documents provided by the customer;

(b) Cross-reference the information provided by the customer with information from other reliable public sources, official websites, and paid databases;

(c) Onsite visits to the customer;

(d) Communicate with the customer via telephone or mail.

(2) Obtain related information for the purpose of insurance purchases and transactions

It is advisable to learn about the customer's purpose of insurance purchases and transactions to determine whether they are reasonable.

(3) Understand the customer's sources of wealth and funding

It is advisable to obtain certificates of wealth (e.g. certificates of bank deposits, salary certificates, deeds, or statements of investment proceeds), financial disclosure statements, and other documents for taking reasonable measures to understand the sources of the customer's wealth and funds as well as the beneficial owners. Source of funds refers to actual sources which generate specific funds (e.g. salary, investment income, purchase and sale of real estate property).

(4) Obtain the approval of senior management personnel

Before establishing or entering a new business relationship, insurance companies are advised to obtain the approval of senior management personnel with the appropriate level of approval authorization based on internal risk considerations.

2. Continuous monitoring of high-risk customers

Insurance companies should adopt the following measures for continuous monitoring of business relationships of high-risk

customers:

(1) Insurance companies should continue to monitor and comprehensively consider the business relationships with customers including customer due diligence, enhanced review of customer information and transaction activities with customers, and pay attention to any changes in transactions or unusual transaction contents.

(2) Insurance companies should verify the names and titles of customers and related transaction counterparties to detect, compare, and screen customers, customers' senior management personnel, beneficial owners, and related transaction counterparties for individuals involved in material cases in media reports, current or former PEPs in domestic and foreign governments or international organizations, individuals, legal persons, or groups designated for sanctions in accordance with the Counter-Terrorism Financing Act, and terrorists or terrorist organizations designated or investigated by foreign governments or international organizations. They shall freeze assets, file suspected ML/TF transaction reports, or take other corresponding risk management measures.

(3) Insurance companies shall conduct periodic reviews (at least once each year) of whether the information obtained for verifying the identity of high-risk customers is sufficient and ensure that updates of such information are provided. They shall also verify the contents of the identity information for processing changes to contracts or insurance payments for high-risk customers.

III. Simplified customer due diligence and continuous monitoring measures

（Ⅰ） Where a customer does not exhibit the aforementioned high-risk

factors or patterns, insurance companies may consider the following low-risk factors and patterns for a comprehensive assessment of low-risk transactions:

1. A customer and related transaction counterparty who are citizens residing within the borders of the Republic of China for long periods of time;
2. A customer who has not appointed an agent or a trustee of a trust to process insurance purchases, claims, contract changes, or other transactions;
3. A customer whose profession does not involve cash-intensive transactions (e.g. general office and field personnel and engineering personnel);
4. A customer whose transaction items do not include cash transactions or cross-border transactions;
5. The insurance products purchased by the customer involves low insurance premiums and no cash value;
6. A customer who conduct transactions through face-to-face sales channels.

（II）Conditions applicable for simplified customer due diligence and continuous monitoring

The following conditions are common low-risk transaction settings in the insurance industry and insurance companies may carry out simplified review and continuous monitoring measures:

1. Where the customer purchases insurance products with no preparatory funds for the insurance value such as short-term life insurance policies, injury insurance, or health insurance;
2. Where the customer purchases small-sum elderly care insurance or micro-insurance;
3. Where the customer purchases group annuity insurance, group periodic life insurance, group injury insurance, group health insurance, and group medical insurance;

4. Where the customer does not exhibit patterns of high ML/TF risks and the insurance premiums for purchased policies does not exceed a certain amount (e.g. NT$30,000) or where single-payment insurance premiums do no exceed a certain amount (e.g. NT$75,000);
5. Other cases deemed by the insurance company as low-risk transactions in accordance with the risk-based approach.

（III） Simplified due diligence and continuous monitoring measures for low-risk customers

Although due diligence procedures cannot be exempted for customers with lower risks, insurance companies may adopt simplified due diligence and continuous monitoring measures:

1. The simplified due diligence and continuous monitoring measures that can be adopted based on insurance companies' risk prevention policies, monitoring and control, and procedures are as follows:
   (1) Reduce the frequency of updating customers' identity information;
   (2) Reduce the level of continuous monitoring measures and adopt a reasonable threshold for the insurance policy preparatory funds or value of accounts as a basis of transaction review.
   (3) If the purpose and the nature of a transaction can be inferred by the transaction type or the existing business relationship, there is no need to collect specific information or carry out specific measures to understand the purpose and the nature of the business relationship.
2. However, the simplified due diligence process cannot be applied to customers who exhibit any of the following circumstances:
   (1) The customer comes from a high-risk country or region

that has not adopted effective anti-money laundering means or means of combating terrorism financing, including without limitation those identified by the FSC and notified to FATF, and other countries or regions which do not comply with or fully comply with the recommendations of FATF.

(2) Where the Bank has sufficient reasons to suspect the customer or transaction is involved in money laundering or terrorism financing activities.

Risk assessment

I. Foreword

Institutions' awareness of risks includes threats and weaknesses. Individual institutions should refer to the criminal pattern reports, threat and risk assessment reports, and statistics published by law enforcement authorities (e.g. Criminal Investigation Bureau of the National Police Agency, Ministry of the Interior, Investigation Bureau of the Ministry of Justice, Customs Administration of the Ministry of Finance, and Agency Against Corruption of the Ministry of Justice) to strengthen their knowledge of suspicious transaction patterns of ML/TF activities that may be carried out in high-threat criminal activity types and by criminals identified in the National Money Laundering and Terrorist Financing Risk Assessment Report. They shall establish individual institutions' knowledge of the patterns of predicate offenses and their use of the insurance system for ML/TF activities in order to strengthen transaction monitoring procedures and the identification of threats based on the National Money Laundering and Terrorist Financing Risk Assessment Report for the purpose of improving the quality of risk assessments for institutions and the

adequacy of customer risk classifications.

When institutions assess inherent risks, it is advisable to conduct assessments on the basis of geography, customers, product and services, transactions, and channels to identify the threats in all aspects before constructing the status of inherent risks of the institution based on an analysis of weaknesses in current laws and company policies. In addition, it is advisable to implement risk reviews at suitable intervals based on the nature and changes of risks (e.g. implement regular reviews, irregular reviews, or both) in order to adopt suitable risk mitigation measures.

II. Geographical risk:

（Ⅰ） Assessment Content

Insurance companies are advised to identify regions with higher ML/TF risks based on the actual operations and experience of their subsidiary companies (or branch companies) while considering their individual requirements (e.g. business development policies) and using the information provided by the Anti-Money Laundering Division of the Investigation Bureau, Ministry of Justice, contents of the National Money Laundering and Terrorist Financing Risk Assessment Report, and information distributed by international anti-money laundering and counter terrorist financing organizations.

（ⅠⅠ）Review frequency

1. Regular reviews: Insurance companies may review and update geographical risks based on the update frequency of their sources of reference information such as quarterly updates of the countries or regions which do not comply, or do not fully comply, with the recommendations of international anti-money laundering organizations as announced by the Financial Action Task Force (FATF).

2. Irregular reviews: Insurance companies shall review geographical risks regularly based on reference sources and they may also use real-time negative news review, National Risk Assessments, and communication with law enforcement agencies (e.g. cases where specific countries or regions are involved in money laundering, terrorist financing, and proliferation of weapons of mass destruction) to assess the geographical risk.

III. Customer risks:

（Ⅰ） Assessment content:

1. Insurance companies may refer to the Anti-Money Laundering Annual Report published by the Anti-Money Laundering Division of the Investigation Bureau, Ministry of Justice, the National Risk Assessment Report published by the Anti Money-Laundering Office of the Executive Yuan, and other official information to understand the threats of criminal activities and industry weaknesses of the insurance industry. They shall also analyze the companies' weaknesses for abuse by customers and consider the background information, nature of professional and socioeconomic activities, organization type and structure of non-natural-person customers, and the customers' transaction amount and methods to identify the customer's ML/TF risks.
2. Insurance companies are advised to include high-risk factors such as whether customers are PEPs, individuals involved in adverse news, non-citizen customers, and high-wealth/net worth individuals into account for the assessment and mitigation of its ML/TF risk exposure.

（ⅠⅠ）Review frequency:

1. Insurance companies are advised to verify customers' identity and assess their ML/TF risks when initiating business

relationships with customers such as purchase of new insurance contracts and changes in contract contents.

2. Insurance companies are required to screen customers' names when they establish business relationships with customers and to conduct regular database name screening to learn about changes in customers' identity and adjust customer risks when required.
3. Insurance companies are advised to perform one regular review for high-risk customers each year. They shall determine the frequency of reviews for customers of other risk ratings in accordance with the risk-based approach identified by individual companies. They shall use the aforementioned regular review procedures to evaluate the customers' motives for purchasing insurance policies, identity, and changes in income status to assess the customer's latest risk rating and determine whether the customer information held by the company is sufficient.
4. Where customers are discovered to be involved in suspected money laundering or terrorist financing transactions, it is advisable to increase the customer's risk rating.

IV. Product and service risks:

（Ⅰ） Assessment content:

Insurance companies may refer to the Anti-Money Laundering Annual Report published by the Anti-Money Laundering Division of the Investigation Bureau, Ministry of Justice, the National Risk Assessment Report published by the Anti Money-Laundering Office of the Executive Yuan, and other official information when they assess product and service risks to understand the threats of criminal activities and industry weaknesses of the insurance industry. they shall also refer to the analyses of high-risk products and businesses specified in the

Industry Risk Assessment Report to understand whether the companies' products are services exhibit the following high risk factors to evaluate the companies' product and service risks: 1. High cash value; 2. Early contract termination; 3. Applicability of policy loans; 4. Diverse source of payment; 5. Complex sources of customers; 6. Short transaction cycles; 7. Ease of purchase or cancellation of policies; 8. Ease of changing the insured.

（II）Review frequency:

1. Insurance companies should perform ML/TF risk assessment when they launch a new product with insurance policy preparatory funds or cash value, services related monetary transactions, or new businesses. It is also advisable to assess potential ML/TF risks of the product in the event of subsequent changes to the content that may cause changes in the characteristics of the product.
2. Insurance companies shall regularly analyze the risk distribution of products purchased by customers and report product contents involved in suspicious transactions. If they discover irregularities such as substantial growth in the number of high-risk products over a s short period of time or certain products that are more susceptible to abuse for money laundering or terrorist financing, they are advised to reassess the risks.

V. Channel risks:

（I） Assessment content:

Insurance companies may refer to the Anti-Money Laundering Annual Report published by the Anti-Money Laundering Division of the Investigation Bureau, Ministry of Justice, the National Risk Assessment Report published by the Anti Money-Laundering Office of the Executive Yuan, and other official

information when assessing channel risks to understand the threats of criminal activities and industry weaknesses of the insurance industry. They shall also consider the companies' use of face-to-face channels (e.g. their solicitors) or non-face-to-face channels (e.g. insurance brokerage or agent companies, online insurance purchases, telephone purchases) to assess the companies' inherent channel risks.

（II）Review frequency:

In addition to conducting regular institutional risk assessments to review the inherent channel risks, it is advisable for insurance companies to conduct regular analysis of the sources of suspicious transaction reports to effectively assess the ML/TF risks of the channels.

VI. Institutional risk assessment

（I） Recommended frequency of institutional risk assessments

1. Insurance companies shall consider the characteristics of their businesses, products, customers, and other factors and establish regular (the recommended frequency is between one to one and a half years) comprehensive ML/TF institutional risk assessments. When insurance companies conduct a comprehensive ML/TF risk assessment, the information obtained from other internal and external sources shall be used as supporting information. Examples include the National Money Laundering and Terrorist Financing Risk Assessment Report published by the competent authority, ML/TF risk information, regulations, and internal audit reports.
2. It is advisable to conduct reassessment procedures in the event of material changes such as items listed below to assess whether the changes affect the overall risks faced by the institution and control measures that should be adopted.

(1) The occurrence of material events or material

developments in management and operations (e.g. corporate mergers or development of cross-border insurance businesses);

(2) When related new threats are generated;

(3) Material penalties for deficiencies in in AML/CFT operations.

（II）Recommended contents of the institutional risk assessment report

1. The institutional risk assessment should provide a comprehensive display of the internal governance framework of the institution, methodology for the execution, risk assessment results, and the measures adopted in response to the risks for the senior management personnel of the board of directors to learn about the risks in businesses and to effectively allocate suitable resources and take effective response measures to prevent or reduce risks. The assessment shall be used to satisfy the requirements for the board of directors to bear ultimate responsibility for establishing and maintaining appropriate and effective AML/CFT internal control.
2. The institutional risk assessment report may be drafted in accordance with the following contents:

(1) Assessment methodology.

(2) Analysis of inherent risks and various control factors and assessment results;

(3) Improvements made previously;

(4) Comparison of assessment results of different periods;

(5) Risk assessment results and residual risk rating of the entire institution;

(6) Risk mitigation measures adopted.

（III） Recommendations for the execution of institutional risk

assessments

1. When establishing the methodology, insurance companies may refer to foreign practical operations and related regulations as well as results of the National Money Laundering and Terrorist Financing Risk Assessment Report or recent regulations for adjustments. The contents, levels, and weights of risk assessment factors may be designed in accordance with the aforementioned contents so that the assessment results fully reflect risks and meet assessment status for ML/TF risks in accordance with international standards.
2. The following measures may be adopted for institutional risk assessment procedures:
   (1) Insurance companies may conduct joint risk assessments with business units that are closely related to AML/CFT operations. The responsible units shall take charge of the implementation status of actual operations to accurately reflect the possible ML/TF threats and weaknesses.
   (2) Before performing risk assessment procedures, responsible units shall participate in meetings with the respective units and clearly define the contents of questions for the assessment. They shall reach a consensus on the contents and prevent errors in risk assessments due to different assessment standards.
   (3) It is advisable to execute the following operations after completing the initial version of the risk assessment report:
      a. The competent units may join business units in assessing whether the contents of risk assessments and scoring and weight design can effectively reflect the risks in the industry and operations.
      b. Verify whether there are deficiencies in internal or

external examinations from the internal risk assessment period to the publication time of the report. If there are deficiencies, it is advisable to include them in the risk assessment and formulate related risk mitigation measures to control and manage risks.

3. After the completion of the risk assessment report, it is advisable to inform the business units and internal audit units of the results. Business units shall adjust operating procedures where appropriate and verify the appropriateness of the operations while internal audit units can also establish related inspection plans based on the assessment results to verify the effectiveness of internal control systems and improve the operations of the three lines of defenses.
4. The results of institutional risk assessments should be explained to related employees through education and training programs for them to understand the weaknesses and threats faced by the company or the industry. They shall use the implementation of functions to effectively reduce ML/TF risks, establish role models, and create a sound corporate AML/CFT culture.

(Ⅳ) Insurance brokers and insurance agents are intermediaries in the insurance industry. Their main risks derive from being used by customers as “launderers” in ML/TF activities. Therefore, insurance brokers and insurance agents should have reasonable knowledge of the risks that are present in their business activities.