Guidance for Insurance Sector on the Best Practices for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Compliance
(Subject: Money Laundering and Risk Management of Counter Terrorism Financing in OIU Business (excluding reinsurance business))

Approved by FSC Letter No. Jin-Guan-Bao-Zong-Zi-10804930210 dated June 24, 2019

Foreword:

These best practices guidance is provided for the reference of insurance enterprises in undertaking anti-money laundering and countering the financing of terrorism (AML/CFT) operation. It is not meant to be mandatory. An insurance enterprise 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.

Risk Management of Money Laundering and Terrorism Financing in OIU Business (excluding reinsurance business)

I. Overview of OIU Business

Since June 2015, various insurance companies have been authorized to start Offshore Insurance Unit (OIU) business by the Financial Supervisory Commission. Compared with other traditional insurance business of insurance companies, the establishing time of OIU business is rather short, and the policy holder and insured are limited to overseas customers, the sources of customers are therefore limited, so the overall operation scale is smaller. The National Money Laundering and Terrorism Financing Risk Assessment Report indicated that the premium income of OIU accounts for a very small proportion of the total premium income, and the number of OIU customers accounts for a very small proportion compared with the number of domestic customers.

II. OIU Money Laundering risk identification

Due to the fact that the OIU business is conducted in foreign currency, that the sales target is primarily offshore customers (including individuals, legal persons, government agencies or financial institutions outside the Republic of China), and that the insurance commodities provided by the current OIU business are mostly high policy value reserves, OIU business therefore have the potential risk of suspicious money laundering transactions.

III. OIU terrorism financing risk identification

OIU business is an insurance business conducted in foreign currencies and sells to overseas customers. Therefore, it can provide funds related to international terrorism activities. However, within those nonprofit corporations that are more likely to be abused in terrorist activities, such as social group, religious nonprofit corporation and social welfare charitable nonprofit corporations, the proportion of such types of customers is very small.

IV. Threat and Vulnerability Identification of OIU

(I) The risk identification and assessment of OIU money laundering and terrorism financing risks should cover four aspects: customer, geography, product and service, transaction and delivery channel. The analysis of risk identification, assessment for each aspect are as follows:

1. Customer risk:

Owing to the limitation of offshore customers, the difference between the acceptance policy of OIU and the traditional insurance business is only the nationality restriction. Nevertheless, offshore customers may still be foreign politically exposed persons or persons with high net worth assets abroad. Since the trading freedom of OIU business is high and the difficulty to obtain and verify information of foreigners, the costs to effectively grasp the true information is high. Therefore there is higher risk using it as a money laundering access. Considering its products policy and customer acceptance policy, the company has to collect information on product categories, transactions and customers, and analyze and evaluate customer sources and risk mitigation measures.

2. Geography risks:

   OIU provides services to offshore customers, who may come from countries around the world, including high-risk countries (regions), countries (regions) with money laundering concerns or tax havens. It is suggested that the following information be used as a basis to identify countries (regions) with higher risk of money laundering and terrorism financing:

   (1) The Financial Supervisory Commission has forwarded the list of that FATF announced that there are significant deficiencies in anti-money laundering and counter terrorism financing, as well as other countries or regions that have not followed or fully followed the recommendations of FATF for the Anti-Money Laundering.
   (2) Countries or regions subject to economic sanctions or other similar measures imposed by the United Nations, the United States or the European Union.
   (3) Countries or regions of offshore financial centers published by the International Monetary Fund.
   (4) Section 311 of the U.S. Treasury Patriot Act designates countries or regions with major money laundering concerns.
   (5) Countries or regions with substantial corruption as listed in the Corruption Perceptions Index of the Transparency International.
   (6) The country or region where the proceeds of crimes described in the national risk assessment report mainly flow into and out of.

3. Product and service risk:

   Customers may utilize the characteristics of insurance products to quickly invest and recover the premiums paid for the circulation of funds by exercising the rights of revocation, termination and borrowing of insurance policies. They may also transfer the value or interests of insurance policies by changing the policyholder or beneficiary.

Currently, OIU mainly provides life insurance products including variable interest rate life insurance, variable life insurance, variable universal life insurance and other savings-type or investment-type insurance products, and is an insurance business that is paid for in foreign currency. And since the interest generated by the investment object or the income from the structured products transaction of the paid premiums and investment-type insurance contract of the business is exempt from withholding income tax, and is essentially more likely to attract overseas customers with different insurance purposes.

Due to the different products policies and customer acceptance restrictions of different companies, the risk situation may be different. It is suggested that insurance companies should timely review the distribution of customers and products (e.g. age, occupation, nationality, etc.) and collect information on product categories, transactions and customers to facilitate timely updating of commodity policies and customer acceptance policies.

4. Transaction and delivery channel risk:

   The OIU business of insurance companies is mostly conducted in person. It mainly provides face-to-face services. Besides through the salesperson of insurance companies, it may also be insured through insurance brokers or insurance agents. In addition, if the company's OIU business can accept international remittances or offshore transactions, it is suggested that relevant enhanced control measures should be adopted to mitigate risks in respect of international remittances or offshore transactions.

(II) Recommendations for identifying threats and vulnerabilities in

OIU business

OIU business is an insurance business, which receives and pays in foreign currency and sells to offshore customers, which transactions involve cross-border services that the authenticity of relevant identity confirmation documents is difficult to identify or need to pay high costs. Our country is a highly developed country in economy and trade, and due to the geographical location, there are countries with frequent criminal incidents and high risk of money laundering and terrorism financing, and such countries are facing criminal threats, which differ from domestic transactions. Therefore, it is suggested that insurance companies should understand the possible threats posed by the relevant trading objects and consider the main criminal threats of their countries (e.g., referring to the relevant analysis of manufacturers in the database, and national money laundering and terrorism financing risk assessment reports published by the countries in questions).

Since the current customer policy of OIU business does not restrict the insurance of foreign political exposed persons or persons with high net worth assets, and the current OIU products are paid for in foreign currencies and have high policy value reserves, it is easier to attract people with a higher degree of involvement in crime to use it as a money laundering tool. Moreover, the authenticity of identity documents provided by foreign customers is difficult to verify and the customers can trade through insurance brokers or insurance agents, and insurance companies are not in direct contact with customers. The aforementioned elements constitute the main vulnerabilities of OIU. In order to enhance insurance companies' understanding of the types of the aforementioned criminal activities and the method criminals conduct suspicious money laundering transactions using OIU business, we can refer to the information of crime pattern reports, threat risk assessment reports and statistics issued by law enforcement agencies such as the Criminal Police Bureau of the Police Department of the Ministry of the Interior and the Investigation Bureau of the

Ministry of Justice, in order to to grasp the information domestically and abroad. Relevant crime trends and investigative experience of law enforcement departments will enhance the understanding of aforementioned criminal patterns and how to engage in money laundering through insurance products.

It is suggested that insurance companies evaluate comprehensively the operating status of OIU business as compared with the overall insurance business (e.g. customer proportion, premium income), the threats faced by OIU (e.g. cross-border services) and the vulnerabilities of OIU business bore (e.g. the difficulty to conduct identity verification). The insurance company shall base risk-based approach to consider the extent of influence from money laundering and terrorism financing risk of OIU business on the entire company and to identify and assess the risk so as to effectively manage and mitigate the identified risks.

The OIU is for offshore customers and the insurance products are paid for in foreign currency. The risk of money laundering and terrorism financing risk exposure is different from other traditional insurance businesses. It is essential to reference the national money laundering and terrorism financing risk assessment reports in view of the aforementioned aspects for identifying and assessing the threats faced by OIU business and concomitantly improve the link between the OIU business and the company's overall risk indicators.

V. Enhance control methods of OIU Business

Since OIU mainly serves offshore customers, whose identity may be foreign political exposed person or a person with high net worth assets, whose place of incorporation may be a high-risk country, a country with money laundering concern or a tax haven, etc. Compared with domestic insurance business, it is more difficult to carry out customer professional authenticity or ultimate substantive beneficiary verification. It is suggested that insurance companies should strengthen the confirmation of the documents, data or information that should be obtained in the process of customer identification. If the customer, based on the risk-based approach, are identified as high-risk customers of insurance companies, the insurance companies should carry out the enhanced due diligence activities. It is also suggested that the customer composition and distribution should be understood in a timely manner by means of customer analysis.

The products offered by OIU business are mostly of high policy value reserve or cash value nature. The insurance premium paid for by OIU business and the interest generated by the investment contract linking the investment object or the gains from the structured commodity transaction are exempted from income tax, therefore it is essentially more likely to attract offshore customers with different insurance purposes. It is suggested that insurance companies should adopt the payment method of bank remittance or transfer to avoid cash flow breakpoint within the cash transactions. If an insurance company triggers a suspicious transaction monitoring alert when conducting customer review or transactions, it shall communicate with law enforcement units in timely manners, and make suspicious transaction declarations or information on the basis of the Money Laundering Control Act and Counter-Terrorism Financing Act.

VI. Strengthening Management Measures of OIU Customers

(I) The documents, data or information suggested to obtain to confirm customer’s identity:

1. When the policyholder and the insured are natural persons:

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

(2) Obtain at least two photocopies of certificates issued by government agencies or other documents with photographs and verify the identity of the holder and his nationality, place of origin or permanent residence.

(3) Obtain signature letters or telephone visits or other authentication measures (e.g. copies of water, electricity, telecommunications, bank bills or tax declaration certificates) with the names and addresses of the insurer and insured depending on the risk level of the clients.

    (4) Obtaining the record of entry into Taiwan at the time of insurance application

2. The policyholder is a legal person:
   (1) Obtain the full name of the legal person, the date and place of registration, the registration number, the address of the place of registration and the address of the principal place of business.
   (2) Certificate of Incorporation issued by the registration authority of the place of registration of the legal person.
   (3) Articles of Incorporation.
   (4) The Certificate of Incumbency issued by the local registration agent of the place of registration of the legal person within 6 months.
   (5) Certificate of Good Standing issued or registered within 6 months of the registration of the legal person's place of registration.
   (6) List of directors, shareholders' registers and senior management.
   (7) The proposer unit should present a copy of the meeting record or authorization letter (with at least the name of the authorized person and the list of insured persons).
   (8) A copy of the identity document of the person in charge or the authorized person.
   (9) Depending on the degree of customer risk, obtain a signed reply letter from the insured person, the name of the insured and the address of the insured, or conduct a telephone interview or other identity verification measures (e.g., photocopies of water, electricity, telecommunications, bank bills or tax declaration certificates.)
3. If the customer is unwilling to cooperate or fail to provide the identity information and verification documents, it is suggested to refuse to establish a business relationship with the customer.

(II) Enhanced customer due diligence and transaction monitoring

If customer is identified as a high risk customer according to the insurance company's risk-based approach, it is necessary to implement enhanced due diligence and take reasonable measures to understand the client's source of wealth and source of funds. It is recommended that the insurance company can refer to the following enhanced customer due diligence measures for OIU customers: The business colleagues should fill out the report, and the customer should fill in the documents such as the insurance, financial notice, and customer suitability assessment to understand the client's entry purpose, identity, insurance motivation, source of funds, cross-matching, understanding the background, and considering the customer's age, job content, and company information are comprehensively evaluated for the products quotas, and insurance motives that are insured. If the documents provided by them are found to be related to money laundering or terrorism financing activities, or when customers review or execute transactions, they may trigger a suspicious transaction monitoring warning. They may communicate with law enforcement units and give feedback in due time, and be prosecuted in accordance with the Money Laundering Control Act and the Counter-Terrorism Financing Act. And respond to suspicious transaction declaration or terrorism financing notification.

(III) Procedures for reconfirming the identity of existing OIU customers

For existing customers before August 18, 2017, the insurance company has completed the process of reconfirming customer identity by requiring the policyholders to provide documents, data or information for verification at the end of 2017. However, if the policyholders fails to complete the data update operation after several notifications, the risk level adjustment will be carried out according to the case data and the transaction situation or the suspicious transaction declaration will be made after the review by the competent supervisor.

VII. Examples of suspected OIU money laundering transactions

When identifying the risk of money laundering, an insurance company may refer to the following examples besides the Appendix: Suspicious Money Laundering or Terrorism Financing Transaction Patterns of Model Notes for Prevention of Money Laundering and Terrorism Financing in the Life Insurance Industry:

(I) The address of the place of registration provided by overseas legal person customers and the address of their main business premises are postal mail boxes.

(II) The client has not fully explained the purpose and motivation of establishing business relations or transactions, or has doubts about the statement of sources of funds.

(III) The substantive beneficiaries of corporate clients/trusts are anonymous shareholders, which makes it impossible to fully identify their ownership structure.

(IV) The large amount of in-bound and out-bound remittances from customer transactions involves a third country other than its place of residence or place of operation, without justifiable reasons.

(V) Payment of individual OIU insurance policy premiums by an overseas legal person account without justifiable reasons.