Guidance for Insurance Sector on the Best Practices for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Compliance (Subject: Suspicious transaction reporting)

Approved by FSC Letter No. Jin-Guan-Bao-Zong-Zi-10704937560 dated July 24, 2018

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.

Suspicious transaction reporting

I. Enhance the effectiveness of monitoring suspicious ML/TF transactions

For the detection of unusual transactions, an insurance company should refer to the red flags for money laundering or terrorism financing transactions set out by the insurance association, and in addition, signs of suspicious activities set by the company itself based on its past experience, and employ information system and manual check in the detection.

II. Suggestions for evaluating suspicious transactions

(I) Consider the situation of individual customers when evaluating the reasonableness of a customer's activities and keep relevant inspection records.

(II) If a customer transaction is suspected of money laundering or terrorist financing following evaluation, the insurance company is advised, after filing a STR with the Investigation Bureau, Ministry of Justice (MJIB), to adjust the risk rating of the reported customer

to high risk to facilitate the system's automatic screening of high-risk customers for subsequent transactions.

(III) If a customer transaction is deemed not suspicious following evaluation, the insurance company should still record the evaluation result and reason for exclusion.

III. Suggestions for enhancing reporting quality and the thoroughness of report

(I) Reasons for filing a STR should cover who, what, when, where, and how. For example, customer identity (background and occupation), and specific irregularities of the unusual transaction (date, amount, transaction frequency or cycle, etc.)

(II) Provide comprehensive supporting information, for example, insurance policy, transaction details or fund transfer details on the unusual transaction.

(III) Communicate and interact fully with the MJIB by, for example, periodically following up on the status of reported cases (under analysis, forwarded to prosecutor's office or put under reference data for the time being) to learn whether the reported data are comprehensive.

(IV) Periodically analyze and review the patterns and types of suspicious transactions. For example, connection with the types of predicate offences for money laundering, the ratio of numbers of actual STR filed to the number of company-wide suspicious transactions under monitoring, and evaluate the reasonableness of the percentage to learn whether there is defensive reporting or whether the conditions set for monitoring are too stringent, and feedback the evaluation findings in a timely manner to adjust the company's reporting rules.

IV. Suggestions for enhancing employees' ability to identify ML/TF risks

To increase the alertness of front-line staff to signs of suspicious transactions and enhance the quality of STR, an insurance company can hold training courses for employees to help them understand matters to pay attention to in filing a STR, promote the importance of suspicious transaction monitoring, and analyze the types of STR filed

by the company in the past.

V. Suggestions for preventing the leak of STR information

(I) Employees at all levels must keep confidential related data of transactions reported to MJIB unless otherwise authorized to disclose.

(II) Related data of reported transactions (e.g. loan repayment details, insurance application, etc.) transmitted via internal email should be encrypted.

(III) Dedicated Unit Officer should authorize the designated personnel to handle suspicious transaction reporting.

(IV) Paper official documents sent to MJIB should be classified confidential and delivered by certified mail.

(V) When filing a STR via media:

1. Filing of a STR must first be approved by the Dedicated Unit Officer or an officer authorized by him/her.
2. IC card and password used for online filing should be kept by different staff.
3. There should be access control in place when the designated personnel files STR via media.