Guidance for Insurance Sector on the Best Practices for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Compliance
(Subject：Managing terrorist financing (TF) risks)

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.

Managing terrorist financing (TF) risks

I. To effectively enhance the management of TF risks, an insurance company can consider the following actions:

(I) Establish an AML/CFT program and implement a training program:

An insurance company should establish an AML/CFT program and carry out employee training on AML/CFT compliance.

(II) Grasp TF threats and trends:

1. Watch closely negative news reports on terrorist financing and grasp timely international trends on combating terrorist financing.
2. Keep abreast of the trend of terrorist organizations raising funds through legal sources or non-profit organizations.
3. Keep abreast of how terrorist organizations using new technologies to raise and transfer funds.

(III) Keep up with the sanction lists:

Visit constantly the AML/CFT webpage of the Ministry of Justice, which has a sanction lists section and allows subscription of electronic notice of updated sanction lists, and pay attention to the updates of sanction lists.

(IV) Build a sanction list database:

An insurance company should not use the externally purchased database as the only source for sanction lists, and is advised to also build its own sanction list database. Upon learning or receiving a list of designated individuals or entities, the company should check if it has been included in the externally purchased database. If not, key it into its own list database. Terrorists or terrorist groups identified or investigated by foreign governments or international organizations should be included in the scope of data to be collected by the database, and the insurance company should pay attention to related transaction risk.

(V) Identify and restrict transactions:

Before establishing business relationship or carrying out a transaction with a customer, an insurance company should identify customer identity. If a customer is confirmed to be on the list of designated individuals or entities, the insurance company may not establish business relationship, nor carry out any transaction with the customer, unless it is otherwise permitted by the TF Review Committee.

(VI) Freeze assets and make a report:

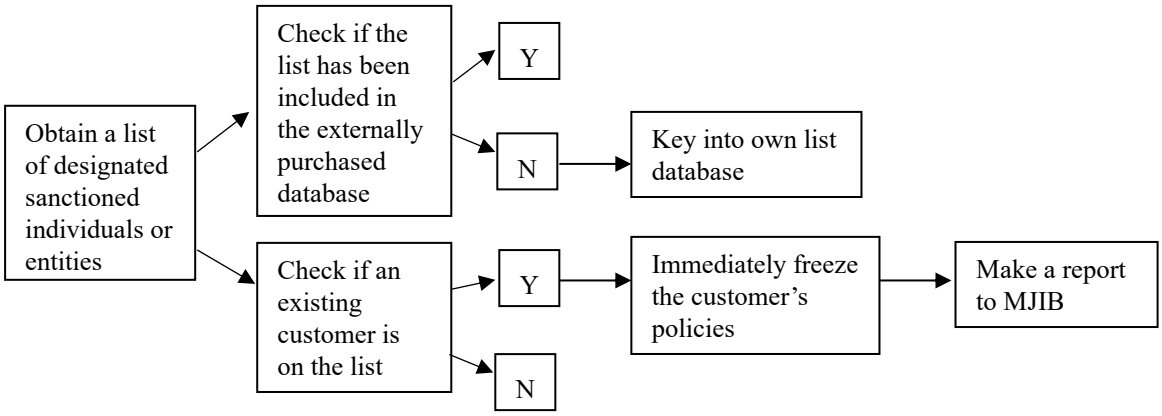
Upon learning or receiving a list of designated individuals or entities, an insurance company should check swiftly if any existing customer is on the list. If yes, the company should immediately freeze the customer’s policies and file a report with MJIB in 10 business days upon discovery.

(VII) Keep related information confidential:

Relevant personnel who learn through business the reporting of properties or property interests and locations of designated sanctioned individuals or entities to MJIB should keep the reporting information confidential.

II. Suggestions for combating the financing of terrorism (CFT) procedure:

(I)



(II)