Financial Holdings Anti-Money Laundering and Countering Terrorism Financing Information Sharing Practice

I. Financial holding companies (hereinafter referred to as “financial holdings”) shall manage the subsidiaries in accordance with the law and establish appropriate internal control systems; also, establish the financial holdings’ overall information sharing policies and procedures for anti-money laundering and countering terrorism financing in accordance with Article 8, Paragraph 10 of the “Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries.” Stipulated the “Financial holdings anti-money laundering and countering terrorism financing information sharing practice” (hereinafter referred to as “the document”) by referring to the Financial Action Task Force (FATF) “FATF Guidance: Private Sector Information Sharing” published in November 2017, the FSC Banking Act No. 10400259730 Letter of the Financial Supervisory Commission dated March 3rd, 2016, and the minutes of meeting of the “Doubts in the Financial Holdings’ Information Sharing Practices” of the Ministry of Justice on January 4th, 2018.

II. The so-called “financial holdings” in the document refers to the financial holding companies and its subsidiaries (hereinafter referred to as the “subsidiaries”) and foreign branches that are subject to the anti-money laundering and countering terrorism financing laws and regulations.

III. For the information sharing of financial holdings, the relevant policies, procedures, and implementation should be planned in accordance with the risk-based approach. The descriptions listed in the document are not the kind of self-regulatory rules established by The Bankers Association of the Republic of China;

therefore, they are without any substantive force of constraint.

IV. The type of information sharing of the financial holdings is illustrated as follows:

1. Due diligence information sharing for existing customers (including beneficial owner)

(1) For the purpose of anti-money laundering and countering terrorism financing, in compliance with the control measures listed in Paragraph 5 of the document, for the due diligence information on the existing customers (including the beneficial owner), the subsidiary may request information sharing within the necessary scope directly from the other subsidiaries or through the financial holdings.

(2) The so-called “due diligence information of existing customers (including beneficial owner)” in the document refers to the information that a subsidiary needs to identify or verify the identity of a customer or a substantial beneficiary in the due diligence of an existing customer, such as : Name (or title), gender, birthday (or date of establishment), email, ID number, occupation, position, employer, nationality, etc.; but does not include customer’s transaction or account information.

2. Information sharing of suspicious transaction reporting

(1) The information of the customer who has been reported as suspected of money laundering transactions may not be clearly shared within the financial holdings. However, if it is included in the list of concerns with the dishonored and high-risk customers or other specific types of lists to avoid any third party can clearly infer that the customer has been declared suspected of money laundering transactions, the list of concerns should be included for information sharing within the banks of the financial holdings.

(2) The information sharing of suspicious transaction reporting or cases helps improve the AML/CFT mechanism of financial institutions, and the suspicious transaction reporting with de-identification can be shared by case or by type.

3. When AML/CFT dedicated personnel and auditors of each subsidiary conducts transaction monitoring, customer due diligence, or related audit, if it is considered involving other subsidiaries and is necessary for further investigation, the AML/CFT dedicated supervisors of other subsidiaries may be requested to provide customers (including beneficial owner) information and their transactions, account information, or other subsidiaries may be suggested to investigate, but should be aware that there must be no violation against the prohibition on the information sharing of the aforementioned suspicious transactions reported.

4. Other related information sharing

   Financing holdings may formulate and share other relevant information in accordance with the risk-based approach and its internal management needs. For example: major negative news and other information related to the anti-money laundering and countering terrorism financing.

V. When supervising the planning of a specific financial holdings' information sharing mechanism, the financing holdings should consider the expected effectiveness and significance of the information sharing mechanism for the financial holdings' anti-money laundering and countering terrorism financing; also, should provide appropriate control measures to the planned specific type of information sharing according to the risk-based approach, such as, but not limited to, the following:

1. Before adopting the specific type of information sharing, the financial holdings should carefully discuss its sharing

procedures and related issues, formulate the sharing process, approval units, and the necessary response measures, and confirm the compliance with the document by the financial holdings' anti-money laundering unit. It should be reported in accordance with the level of information security shared to be approved by the appropriate authority within the financial holdings. For customer (including beneficial owner) due diligence information sharing between subsidiaries, it shall be handled only after the approval of the financial holdings' anti-money laundering director, except for the public information, known facts, or educational training messages not involving the customer.

2. If the financial holdings' information sharing involves the information of the customer or its substantial beneficiary, the financial holdings should require the subsidiary to adopt appropriate measures, such as: Authority control, file independence, etc., to prevent information from being used for purposes other than anti-money laundering and countering the financing of terrorism. Also, the subsidiary should be required to adopt appropriate security measures to prevent the above information from being stolen, falsified, damaged, lost, or leaked. In order to enhance the effectiveness of security measures, financial holdings shall require the subsidiaries that participate in this information sharing to have a security and confidentiality agreement signed, including the confidentiality obligation to reaffirm the prohibition of the disclosure of suspicious transaction declarations that must be implemented truthfully.

3. When handling information sharing, financial holdings should pay attention to the use of information equipment, internet, or technology; also, take into account the timeliness, convenience, and security of information to ensure the

integrity and security of information transmission.

4. In order to strengthen the effectiveness of the information sharing process of the financial holdings, the financial holdings should handle relevant education and training, such as, the purpose and effectiveness of information sharing, sharing information confidentiality and information security, sharing operations and process promotion, etc.

5. The anti-money laundering unit of the financial holdings shall formulate the relevant financial holdings' information sharing procedures; also, report to the President of the financial holdings at least every six months on the content and effect of the implementation within the financial holdings. If there is customer due diligence information sharing between subsidiaries (including beneficial owner), the implementation status should be reported to the Board of Directors at least every six months.

VI. When the information sharing in the financial holdings involves a foreign subsidiary or a foreign branch, it must be in compliance with the local information confidentiality provisions of the subsidiaries (or branches) in Taiwan and abroad. If it intendeds to provide information to the subsidiary or the branch abroad, ensure that it is not used for anything other than the intended purpose.