Annex

Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control Programs by Electronic Payment Institutions

Financial Supervisory Commission on July 03, 2015
FSC.Banking.Bills.Tzi No. 10400111140 Letter approved for future reference
Financial Supervisory Commission on September 30, 2017
FSC.Banking.Bills.Tzi No. 10600225010 Letter approved for future reference

I. The "Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control Programs by Electronic Payment Institutions" is enacted in accordance with the "Directions Governing Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business, Electronic Payments Institution, and Electronic Stored Value Card Issuers" for the purpose of anti-money laundering and countering terrorism financing. It covers the subjects of "how electronic payment institutions in Taiwan recognize and assess the money laundering and terrorism financing risks" and with the anti-money laundering and countering terrorism financing programs enacted for reference in implementation.

II. The risk control mechanism or internal control system of an electronic payment institution shall be approved by the Board of Directors (Executives), same for the amendment. Its contents should include the identification, assessment, and management of the money laundering and terrorism financing risks, the stipulation of the related written policies and procedures, the anti-money laundering and countering terrorism financing program formulated in accordance with the risk assessment result, and a

regular review.

A risk-based approach is designed to assist in the development of a control and counter measure that is commensurate with the money laundering and terrorism financing risk in order to help electronic payment institutions determine the allocation of anti-money laundering and countering terrorism financing resources, establish an internal control system, and stipulate and implement the policies, procedures, and control measures of an anti-money laundering and countering terrorism financing program.

The instructions cited in the "Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control Programs by Electronic Payment Institutions" are not mandatory norms. The risk assessment mechanism of the electronic payment institutions should be commensurate with the nature and size of the business operations. For smaller or simpler electronic payment institutions, a simple risk assessment is sufficient; however, for electronic payment institutions with complex products and services and with a wide range of products provided by multiple branches (or subsidiaries) or with the products and services used by diversified users, a higher degree of risk assessment procedure should be performed.

III. Electronic payment institutions should take appropriate measures to identify and assess their money laundering and terrorism financing risks; also, base on the specific risk assessment items that are determined according to the identified risks to further control, reduce, or prevent such risks.

The specific risk assessment items should include at least the geography, users, products and services, transaction or payment pipeline, etc., and

should further analyze each risk item to stipulate detailed risk factors.

(I) Regional risk:

1. Electronic payment institutions should identify the areas at higher risk of money laundering and terrorism financing.
2. In setting a list of regions with high risk of money laundering and terrorism financing, electronic payment institutions may choose the applicable reference criteria based on the actual experience of their respective branches (or subsidiaries) or by referring to the appendix, and taking into account the individual needs.

(II) User risk:

1. Electronic payment institutions should consider the personal user's background, occupational and socio-economic characteristics, geographical areas, and the organization and structure of non-personal users to identify the users' money laundering and terrorism financing risks.
2. In identifying personal users' risks and determining their risk level, the electronic payment institutions should base their assessment on the following risk factors:
   (1) Geographical risk of users: Base on the list of areas with the risk of money laundering and terrorism financing defined by the electronic payment institutions to assess the user's nationality and country of residence risk.
   (2) Occupation and industry money laundering risk of Category III electronic payment account users: Base on the money laundering risk of each occupation and industry defined by the electronic payment institutions to assess the user's occupation and industry risk. High-risk industries refer to the companies or trusts engaged

in cash-intensive business transaction or those easily being used to hold personal assets.

(3) User registration channels

(4) Trading limits for each type of electronic payment account

(5) Whether the users are with other signs of high money laundering and terrorism financing risks, such as, the user is a foreigner without a residence permit or non-resident national who does not hold a residence registration and cannot give reasonable explanations; the user is a company and an anonymous shareholder or a company that can issue bearer stock shares; the complexity of the shareholdings of corporate user, such as, the obvious abnormality of the shareholding structure or the high complicity of the shareholding structure comparing to its business nature.

(III) Product and service, trading, or payment pipeline risk:

1. Base on the nature of each product and service, trading, or payment pipeline to identify those with high risk of money laundering and terrorism financing.
2. Conduct comprehensive money laundering risk assessment before launching a new product, service, or distribution network, and establish a corresponding risk management measure to mitigate the identified risks in accordance with the principle of risk control.
3. Individual product and service, trading, or payment pipeline risk is illustrated as follows:

(1) It is not easy to trace the source of funds or difficult to identify identity.

(2) Cash out operation.

(3) Is it a large amount or high value transfer operation?

(4) Anonymous trading.

(5) Received money from unknown or unrelated third parties.

IV. Electronic payment institutions should establish different user risk levels and classification rules.

The user risk level should include at least two risk levels (inclusive), that is, "high risk" and "general risk" as the basis for enhanced due diligence and the continuous monitoring mechanism implementation. For electronic payment institutions with only a two-level risk rating, the "general risk" rating is higher than the "low-risk" rating as indicated in Points 5 and 7 of the "Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control Programs by Electronic Payment Institutions;" therefore, a simple measure is not applicable to the user with "general risk."

Electronic payment institutions shall not disclose the user's risk level information to the user or other persons who are not involved in the implementation of anti-money laundering or countering terrorism financing obligations.

V. Except for the politically exposed persons of a foreign government and those who faced economic sanctions, terrorists or terrorism group charged or traced by foreign governments or by the International Money Laundering Prevention Organization, and the individuals, legal persons, or groups designated by the Terrorism Financing Control Act for sanctions shall be directly considered as high-risk users, the electronic payment institutions should set the types that should be directly considered as high-

risk users according to their business models and considering the relevant risk factors.

Electronic payment institutions may define their own types of users that are directly considered as low-risk users based on the complete written risk analysis. The written risk analysis results should be sufficient enough to demonstrate that these types of users are commensurate with the lower risk factors.

VI. For newly registered users, the electronic payment institutions shall determine their risk level within 60 days after accepting the registration.

For the existing users with a defined risk level, the electronic payment institutions shall re-conduct the user risk assessment in accordance with their risk assessment policies and procedures.

Although the electronic payment institutions have conducted risk assessments on users when accepting their registrations, for certain users, the overall risk profile of the users will not be clarified until the users make transactions through an account. Thus, the electronic payment institutions should review the identity data of the existing users in accordance with the importance and degree of risk. After considering the timing of the last user review and the adequacy of the information obtained, the electronic payment institutions shall review the existing relationships at an appropriate time and adjust the user's risk level accordingly. The aforementioned appropriate timing shall include at least:

(I) When users apply for a new electronic payment account.

(II) Periodic reviews are determined in accordance with the importance and risk level of the user.

(III) When there is a significant change in user identity and background

information.

(IV) When reporting a suspected money laundering or terrorism financing transaction, an event that may lead to a material change in the user's risk profile occurs.

Electronic payment institutions should periodically review the sufficiency of the information they have acquired to verify the user's identity and ensure having such information updated, particularly for high risk customers; also, the electronic payment institutions should have it reviewed at least once a year.

VII. Electronic payment institutions should establish corresponding control measures based on the identified risks in order to reduce or prevent the money laundering risks. Electronic payment institutions shall determine the respective control measures applicable to users with different risk levels accordingly.

For the risk control measures, electronic payment institutions should adopt different control measures based on their risk control policies, monitoring, and procedures for different types of high-risk users and those with specific high-risk factors in order to effectively manage and reduce the known risks as follows:

(I) Enhanced Due Diligence, for example:

1. Obtain the relevant information about the purpose of applying for registration and purpose: such as, the purpose of an electronic payment account and expected user transaction activities.
2. Obtain further business information from users: Learn about user business contacts.
3. Obtain instructions and information on the transaction to be completed or already completed.

4. Conduct a field visit or telephone interview according to the type of users in order to confirm the actual operation of the user.

(II) Obtain the approval of higher management.

(III) Increase the frequency of user due diligence.

(IV) Enhanced monitoring mechanism

For low-risk situations, electronic payment institutions should take simplified measures based on their risk control policies, controls, and procedures.

VIII. Electronic payment institutions should establish regular and comprehensive risk assessment activities for money laundering and terrorism financing, and prepare risk assessment reports so that the management can understand the overall risk of money laundering and terrorism financing faced by the electronic payment institutions in a timely and effective manner in order to determine the mechanism to be established and to develop appropriate counter measures.

Electronic payment institutions should establish regular and comprehensive money laundering and terrorism financing risk assessment operation based on the following indicators:

(I) The nature, scale, diversity, and complexity of the business operation

(II) Targeted market

(III) Electronic payment institutions trading volume and size: Consider the general trading activities of the electronic payment institutions and the characteristics of the users.

(IV) High risk related management data and reports: such as, quantity and ratio of high risk users; the amount, quantity, or ratio of high risk products, services, or trade amount; user’s nationality, place of

incorporation or place of business, or amount or ratio of the transactions involving high risk areas.

(V) For business and product, it includes the ways and means of providing services and products to users, means of conducting user due diligence, such as, the extent to which information systems are used and whether or not to entrust a third party to conduct a review.

(VI) Internal audit and the inspection results of the competent authorities

In conducting the comprehensive risk assessment of money laundering and terrorism financing operations in the preceding paragraph, in addition to considering the aforementioned index, the electronic payment institutions propose to refer to the information obtained from other internal and external sources, such as:

(I) Management reports provided by internal management of the electronic payment institutions (such as, business unit managers, user relationship managers, etc.)

(II) Anti-Money Laundering and Countering Terrorism Financing Report issued by International Anti-Money Laundering Organizations and other countries.

(III) The information on the money laundering and terrorism financing issued by the competent authorities

The comprehensive money laundering and terrorism financing risk assessment results of the electronic payment institutions should be used as the basis for the development of anti-money laundering and countering terrorism financing programs. Electronic payment institutions should allocate appropriate manpower and resources based on the risk assessment results and take effective countermeasures to prevent or reduce the risk.

Electronic payment institutions while experiencing major changes, such as,

major events, significant developments in management and operations, or emerging of new threats related to major changes should have the assessment operation initiated again.

When the risk assessment report is completed or updated, the electronic payment institutions shall submit the risk assessment report to the Financial Supervisory Commission (hereinafter referred to as the "FSC") for reference. The sideline electronic payment institutions shall also handle it in accordance with the relevant industry provisions.

IX. The policies of the electronic payment institution that are enacted in accordance with the "Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control Programs by Electronic Payment Institutions" should be implemented with the approval of the Board of Directors (Executives); also, it should be submitted to the Financial Supervisory Commission for future reference along with the Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Electronic Payment Institutions (Template); also, it should be reviewed annually. The same for the amendments.