The Bankers Association of the Republic of China Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Electronic Payment Institutions (Template)

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

Article 1

The "Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Electronic Payment Institutions (Template)" is enacted in accordance with the "Money Laundering Control Act," "Terrorism Financing Control Act," "Regulations Governing Anti-Money Laundering of Financial Institutions" and "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 preventing money laundering and combating the financing of terrorism (hereinafter referred to as the "prevention of money laundering and the fight against terrorist financing").

Article 2

The risk control mechanism or internal control system established in accordance with Article 33 of the "Rules Governing Internal Control and Audit System of Electronic Payment Institutions" shall be approved by the Board of Directors (Executives), same for the amendments. The contents shall include the following:

I. Base on the "Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control

Programs by Electronic Payment Institutions" (Annex) to formulate the relevant policies and procedures for the identification, assessment, and management of money laundering and terrorism financing.

II. Formulate an anti-money laundering and countering terrorism financing program in accordance with the "Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control Programs by Electronic Payment Institutions," the results of the risk assessment, and the scale of business operations to manage and mitigate the identified risks and take greater control over the higher risks involved.

III. Supervise and control the compliance of anti-money laundering and countering terrorism financing and the standard operating procedures for anti-money laundering and countering terrorism financing program implementation with the self-checking and internal audit items included and enhanced, when necessary.

The identification, assessment, and management of money laundering and terrorism financing in Section 1 of the preceding paragraph shall at least cover the user, geographical area, product and service, transaction or payment pipeline, etc.; also, it shall be conducted in accordance with the following provisions:

I. A risk assessment report should be prepared.

II. All risk factors should be considered in order to determine the overall risk level and the appropriate measures for mitigating the risk.

III. A mechanism for updating the risk assessment report should be established to ensure the updating of risk information.

IV. The risk assessment report should be submitted to the Financial Supervisory Commission (hereinafter referred to as the "FSC") for

future reference when it is completed or updated.

The Anti-Money Laundering and Countering Terrorism Financing Program referred to in Section 2, Paragraph 1 shall include the following policies, procedures, and control measures:

I. Confirmation of user identity.

II. Checking User's name and title.

III. Continuously monitoring accounts and transactions.

IV. Records keeping.

V. Reporting currency transactions that exceed a certain amount of money.

VI. Reporting suspected money laundering or terrorism financing transactions in accordance with the Terrorism Financing Control Act.

VII. Appointing the functional head who is in charge of anti-money laundering and countering terrorism financing to be responsible for compliance matters.

VIII. Staff selection and appointment procedure.

IX. Continuous staff training program.

X. The independent auditing function for testing the effectiveness of the anti-money laundering and countering terrorism financing system.

XI. Other matters in compliance with the relevant laws and regulations on anti-money laundering and countering terrorism financing and the requirements of the Financial Supervisory Commission.

An electronic payment institution with a foreign branch (or subsidiary) should set up a group-level anti-money laundering and countering terrorism financing program to be implemented within the branches (or subsidiaries) of the group. In addition to the policies, procedures, and control mechanisms stated in the preceding paragraph, the following matters

should be enacted in compliance with the data confidentiality requirements of Taiwan and the foreign countries where the branches (subsidiaries) located:

I. The internal information sharing policies and procedures needed for confirming the user identity and the money laundering and terrorism financing risk management

II. For the purpose of anti-money laundering and countering terrorism financing, when necessary, request foreign branches (or subsidiaries) to provide information on the relevant users, accounts, and transactions in accordance with the group-level compliance, audit, and anti-money laundering and countering terrorism financing functions.

III. Security for the use of the exchanged information and its confidentiality

Electronic payment institutions should ensure that their foreign branches (or subsidiaries) implement anti-money laundering and countering terrorism financing measures consistent with the head office (or parent company) subject to the local law and regulations. When the minimum requirements of the nations where the head office (or the parent company) and the branch (or subsidiary) located are different, the branch office (or subsidiary) should comply with the higher standard of the two nations. In case of doubt regarding the higher standards of the two nations, the determination of the competent authority of the country where the head office (or the parent company) of the electronic payment institutions located shall prevail. When the same standards as the head office (or parent company) cannot be adopted due to the prohibition of foreign laws and regulations, adequate additional measures should be adopted to manage the risk of money laundering and terrorism financing; also, it should be

reported to the Financial Supervisory Commission.

For the money laundering and terrorism financing risk identification, assessment, and management related policies and procedures; also, the policies, procedures, and control mechanism included in the anti-money laundering and countering terrorism financing program 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" by the branches or subsidiaries of a foreign financial institution in Taiwan as stated in Section 1 and Section 2, Paragraph 1, if the parent group has them established not inferior to the requirements of Taiwan without violating the laws and regulations of Taiwan, such branches or subsidiaries in Taiwan may apply the same requirements of the parent group.

The Board of Directors (Executives) of the electronic payment institutions is ultimately responsible for ensuring the establishment and maintenance of appropriate and effective internal control for anti-money laundering and countering terrorism financing. The Board of Directors (Executives) and senior management shall understand the risks of money laundering and terrorism financing, the operation of anti-money laundering and countering terrorism financing program, and adopt measures to shape the culture of appreciating the importance of anti-money laundering and countering terrorism financing.

Article 3

The terminologies included in the Template are as follows:

I. A certain amount of money: NT$500,000 (including equivalent value in foreign currency).

II. Currency transactions: It refers to one single transaction of cash

received or paid (it refers to all cash receipt and payment vouchers in accounting process)

III. Establishing a business relationship: It refers to the timing when the electronic payment institutions accepting the user's application for registration.

IV. Electronic Payment Institutions: It refers to the franchised electronic payment institutions and the banks engaging in the business of electronic payment institutions, Chunghwa Post Co., Ltd., and Electronic Stored Value Card Issuers.

V. Electronic payment account: It refers to the electronic payment institutions accepting the users to open a network account for recording transfer of funds or stored value.

VI. Users: It refers to the registration with the electronic payment institutions and opening an electronic payment account in order to utilize the service provided by the electronic payment institutions for transfer of funds and stored value.

VII. Personal users: It refers to the natural persons, including foreign natural persons and natural persons in Mainland China.

VIII. Non-personal users: It refers to the government agencies, legal persons, companies, other groups of Taiwan, and foreign legal persons and legal persons in Mainland China.

IX. Real beneficiary: It refers to a natural person who has ultimate ownership or control, or a natural person who trades through an agent, including a natural person who has ultimate and effective control over a legal person or legal agreement.

X. Risk-based approach: An electronic payment institution should confirm, assess, and understand the money laundering and terrorism

financing risk it exposed to and should adopt appropriate anti-money laundering and countering terrorism financing measures to effectively reduce such risks. According to the risk-based approach, an electronic payment institution should take a more stringent measure against higher risk and take a relatively simplified measure against lower risk in order to effectively allocate resources and reduce the identified money laundering and terrorism financing risks with the most appropriate and effective measure.

Article 4

The confirmation of user identity should be handled in accordance with the following provisions:

I. Decline establishing a business relationship or transaction with the user in any of the following situations:

(I) Suspected of using an anonymous, pseudonym, head, dummy company, or dummy legal person group.

(II) Users refuse to provide relevant documents for verifying the users' identity, except for those who have been verified with a credible and independent source.

(III) In the case of an electronic payment account or transaction registered by an agent with difficulty in verifying the fact of the agency and the identity of the agent.

(IV) Possess or use a false or altered identity document.

(V) Present proof of identity copies for an application filed over the counter. Except for businesses that can be processed with proof of identity copies or video files according to the law and regulations, along with the use of other control measures.

(VI) Provide suspicious or obscure documents and are unwilling to provide other supporting data or the provided data is unable to be verified.

(VII) Users unusually delay in providing supplementary identity documents, registration certificates, or related documents approved.

(VIII) The business counterparty is an individual, legal person, or group designated for sanctions under the Terrorism Financing Control Act, and terrorists or groups identified or traced by foreign governments or international organizations. Except for payments made under Sections 2-4, Paragraph 1, Article 6 of the Terrorism Financing Control Act.

(IX) The same financial payment instrument that has been provided for identity verification is repeatedly provided by different users for identity verification.

(X) The relevant authority reports that the user has a record of illegally using the deposit account or electronic payment account of a financial institution.

(XI) Other applications filed for registration are declined according to the requirements of the competent authority.

II. Timing for the confirmation of user identity:

(I) At the time of establishing a business relationship between the electronic payment institutions and users.

(II) At the time of conducting a currency transaction for a certain amount of money.

(III) The electronic payment institutions when implementing the ongoing due diligence should perform the identity confirmation procedure again in any of the following situations:

1. Personal users and non-personal users respectively apply for changing the basic identity information as stated in Article 7 and Article 11 of the "Regulations Governing Identity Verification Mechanism and Transaction Limits for Users of Electronic Payment Institutions."
2. Anomalies occurred in the transaction of user's electronic payment account.
3. Documents, such as, identity documents or registration certificates, provided by the users upon registration may be counterfeit or altered.
4. User's current trade is more than one (1) year from the previous transaction.
5. The same mobile phone number is used by different users for identification procedures.
6. Discover suspected money laundering or terrorism financing transactions, or discover deposit transactions made from a country or region with high risk of money laundering or terrorism financing.
7. The authenticity or fitness of the user's identity information obtained is in doubt.
8. The electronic payment institutions according to obvious evidence believe that it is necessary to confirm the identity of the user again.

III. The confirmation of user identity should be handled in accordance with the following provisions:

(I) When establishing the business relationship with the user, the electronic payment institutions shall handle it in accordance with

the relevant provisions of the "Regulations Governing Identity Verification Mechanism and Transaction Limits for Users of Electronic Payment Institutions."

(II) In the case of a business relationship established by an agent, the fact of the agency should be verified and the identity of the agent should be identified and verified according to the existing method and with the photocopy of the identity document or record kept.

(III) If the non-personal user of Category III electronic payment account is a legal person, the real beneficiary of the user must be confirmed and its identity is to be verified with reasonable measures, including the use of reliable sources of data or information.

(IV) The measures used to confirm user identity should include understanding the purpose of establishing a business relationship and obtaining the relevant information as appropriate.

(V) Identify and confirm the user identity information again, in addition to checking the identity documents, registration documents, and other relevant documents, it can be handled as follows:

1. Request users to submit additional identity information.
2. Contact the user by phone, email, or in writing.
3. Visit users in person.
4. Verify with the relevant institutions.

(VI) For those users who failed to cooperate with the repeating identity verification and confirmation as stated in Item 3, Section 2 and the preceding section, their trading functions shall be

suspended according to the contractual agreement.

IV. When the users as stated in Section 3 are non-personal users, try to understand the business nature of the users and the business purpose of the non-personal users outside the country.

V. When the non-personal user of Category III electronic payment account is a legal person, the real beneficiary of the user must be confirmed with the following information:

(I) The identity (e.g. Name, date of birth, nationality, identity card number, etc.) of the controlling ultimate natural person The aforementioned "control" refers to the holding of more than 25% of the shares or capital of the legal person.

(II) If no controlling natural person is found or whether the controlling natural person is a real beneficiary is doubtful, check whether there is a natural person who exercises control over the user through other means. If necessary, obtain a statement from the user to confirm the identity of the real beneficiary.

(III) In the absence of any foreseeable natural person identified as stated in the last two Sub-Item, reasonable measures should be taken to ascertain the identity of a natural person in a senior management position (such as, a director or general manager or other person having a comparable or similar title).

(IV) Users or controlling persons with any of the following identities, except for the proviso stated in Section 3, Paragraph 1, Article 6, are not subject to the aforementioned requirements of identifying and confirming the identity of the real beneficiary:

1. Government agencies of Taiwan, ROC;
2. State-run business institutions of Taiwan, ROC;

3. Government agencies of foreign government;

4. Public offering company or its subsidiaries in Taiwan;

5. The listed/OTC companies or their subsidiaries listed offshore with the major shareholders disclosed in accordance with the requirements of the local authorities;

6. The financial institutions supervised by the authorities of Taiwan and their investment instruments;

7. The financial institutions established offshore under the governing specifications that are consistent with the anti-money laundering and countering terrorism financing standards enacted by The Financial Action Task Force on Money Laundering (FATF), and the investment instruments managed by such financial institutions; Electronic payment institutions shall keep relevant documents (such as, public information check records, rules and regulations on anti-money laundering of the financial institutions, negative information query records, financial institution declarations, etc.) on the aforementioned financial institutions and investment instruments.

VI. Users who are identified as high-risk or with specific high-risk factors according to the rules governing money laundering and terrorism financing risk assessment of electronic payment institutions should be verified with more stringent measures adopted, such as:

(I) Obtain a reply letter countersigned by the authorized representative of the principal/legal person or group that was mailed to the address indicated by the users, or arrange a phone interview.

(II) Obtain supporting document of the fund sources and fund use of

the legal person and group, such as, the list of major suppliers, the list of main users, etc.

(III) Field visits

VII. For the users who are identified as high-risk or with specific high-risk factors according to the rules governing money laundering and terrorism financing risk assessment of electronic payment institutions, the electronic payment institutions upon confirming the identity of the user should make use of the electronic payment institution's own database or external information sources to check whether the users and their real beneficiaries and senior management are or were politically exposed persons of Taiwan, foreign governments, or international organizations.

(I) If the users or their real beneficiaries are politically exposed persons of a foreign government, the users shall be regarded as high-risk users directly and shall take measures as stated in each item of Section 1, Paragraph 1, Article 6 to confirm the identity of the customers forcefully.

(II) If the users or their real beneficiaries are politically exposed persons of Taiwan or international organizations, the related risks shall be reviewed at the time of establishing a business relationship with the users and they shall be reviewed again annually. Users identified as with high-risk by electronic payment institutions are subject to the identity confirmation process with the stringent measures stated in each item of Section 1, Paragraph 1, Article 6.

(III) If the senior management of a user is an politically exposed person of Taiwan, a foreign government, or an international

organization, the electronic payment institutions shall consider the influence of the senior manager on the user and decide whether the user is subject to the identity confirmation process with the stringent measures stated in each item of Section 1, Paragraph 1, Article 6.

(IV) For those who are currently not an politically exposed person of Taiwan, a foreign government, or an international organization, the electronic payment institutions should consider the relevant risk factors and then assess its influence, and base on the risk-based approach to determine whether it is subject to the provisions in the last three items.

(V) The provisions of the last four items are applicable to the family members or closely related persons of the said politically exposed persons. The aforementioned family members and those who are closely related shall be determined in accordance with Paragraph 4 (the last paragraph), Article 7 of the Money Laundering Control Act.

(VI) For the individuals stated in Sub-item 1 to 3, Item 4, Section 5, if third real beneficiaries or senior management personnel are politically exposed persons, they are not subject to the provision of Item 1 to 5 of this Section.

VIII. Other compliance matters for the confirmation of user identity:

(I) Without prejudice to the relevant laws and regulations, electronic payment institutions should not accept or should cut off business relationships if they know or must assume that users' funds come from corruption or abuse of public assets.

(II) Electronic payment institutions should confirm and record the

users' identity according to the government-issued or other identification documents when establishing business relationships with the users or when the users' information is not sufficient enough to confirm their identity.

(III) For the users in doubt with a business relationship established through commission or after a business relationship established, confirm their identities by telephone, in writing, or a field visit.

(IV) Electronic payment institutions should consider reporting any suspicious money laundering or terrorism financing transactions of the users if they failed to complete the relevant procedures of identity confirmation.

(V) If an electronic payment institution suspects that a user or transaction may involve money laundering or terrorism financing, and reasonably believes that performing identity confirmation procedure may reveal such information to the user, the electronic payment institution may report a suspected money laundering or terrorism financing transaction instead of performing the said procedure.

(VI) Other matters needing attention while establishing a business relationship should be handled in accordance with the internal operating requirements of the electronic payment institutions.

IX. The following situations may be handled in accordance with the contractual agreement as follows:

(I) For the matters stated in Item 8, Section 1, the electronic payment institutions may have the users suspended from using the services provided by the electronic payment institutions or may have the contract terminated.

(II) For those who do not cooperate with the confirmation or re-confirmation of identity, refuse to provide information on the real beneficiaries or the individuals who exercise power over the users, refuse to explain the nature and purpose of the transaction or the source of funds, or there are sufficient evidences proving the user's using the electronic payment account to commit frauds, money-laundering, or suspected wrongdoings, the electronic payment institutions may suspend the users from using all or part of the business services or may have the contract terminated for any serious nonconformity committed.

X. Where a business relationship or trade counterparty is established as described in Item 8, Section 1, electronic payment institutions shall report the suspected money laundering or terrorism financing transactions in accordance with Article 10 of the Money Laundering Control Act. If the trade counterparty is the individual, legal person, or group designated for sanction as stated in the Terrorism Financing Control Act, the electronic payment institutions may not commit any acts that are stated in Paragraph 1, Article 7 of the Terrorism Financing Control Act starting from the date of their knowledge; also, it should be reported in accordance with the provisions of the Terrorism Financing Control Act(please have the form downloaded from the website of the Investigation Bureau, Ministry of Justice). If the electronic payment institutions have committed any of the matters stated in Section 3 and 4, Paragraph 1, Article 6 of the Terrorism Financing Control Act before the aforementioned parties subject to sanction, an application should be filed with the Terrorism Financing Committee in accordance with the relevant ordinances of the

Terrorism Financing Control Act.

Article 5

The measures adopted by the electronic payment institutions for confirming user identity should include the ongoing due diligence for user identity and it should be handled in accordance with the following provisions:

I. Review the transactions conducted with the users in details to ensure that the transactions undertaken are consistent with the users' businesses and risks; also, where necessary, understand their sources of funds.

II. Regularly review whether the information obtained for identifying the identity of users and their real beneficiaries is sufficient enough or not, and ensure having such information updated, especially for high-risk users, they should be reviewed at least once a year. In addition to the aforementioned users, the frequency of review should be determined according to the risk-based approach.

III. User identity identification and verification procedures can be based on previous executions and preservation of data without having the user identity identified and verified repeatedly for each transaction engaged. However, if the electronic payment institutions are suspicious of the authenticity or appropriateness of the user information, find that the user is involved in any suspected money laundering or terrorism financing transaction, or the user's transaction or the operation of the account is subject to significant changes that do not conform to the user's business features, the identity of the user shall be reconfirmed in accordance with the provisions of Article 4.

Article 6

The level of due diligence for the user identity confirmation measures and ongoing due diligence stated in Section 3, Article 4, and Article 5 should be determined in accordance with the risk-based approach, including:

I. Implement enhanced due diligence or ongoing due diligence for users with high-risk situations, of which, at least with the following enhanced measures adopted additionally:

(I) Before establishing or adding a business relationship, the electronic payment institutions shall obtain the approval of the senior management that is authorized according to the internal risk considerations.

(II) While performing the ongoing due diligence for the users of Category III electronic payment account, adopt reasonable measures to understand the wealth of the users and the source of funds. The source of funds refers to the real source of the funds (such as, salary, investment income, real estate trade, etc.).

(III) The business relationship shall be supervised forcefully and continuously.

II. Adopt enhanced measures commensurate with the risk of the users who are from the countries or regions with high risk of money laundering or terrorism financing.

III. For a lower risk scenario, simplified measures shall be adopted, which shall be commensurate with the lower risk factors. However, simplified measures shall not be adopted for the confirmation of user identity in the following circumstances:

(I) For users from countries or regions that have not taken any effective measures to prevent money laundering or terrorism

financing, the said high-risk countries or regions refer to the countries or regions with a serious nonconformity in anti-money laundering and countering terrorism financing committed that are announced by International Anti-Money Laundering Organizations and forwarded by the Financial Supervisory Commission.

(II) The users or transactions are suspected of money laundering or terrorism financing.

The simplified measures for the confirmation of user identity available to the electronic payment institutions are as follows:

I. Reduce the frequency of user identity data update.

II. Reduce the level of continuous monitoring and use a reasonable threshold amount as a basis for reviewing the transaction.

III. If the purpose and nature can be inferred from the type of transaction or the established business relationship, it is not necessary to collect specific information or to carry out special measures for the need of understanding the purpose and nature of the business relationship.

Electronic payment institutions should review 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.

Article 7

Electronic payment institutions should handle the user identity confirmation on its own initiative. If it is otherwise provided by law or the competent authority that the electronic payment institutions may rely on the

third party to identify and verify the identity of the user or the user's representative, the identity of the agent, the entity of the real beneficiary, or the purpose and nature of the business relationship, the electronic payment institutions that has the third party commissioned are still ultimately responsible for the confirmation of user identity and shall meet the following requirements:

I. Should be able to immediately obtain the information needed for confirming the identity of the user.

II. Adopt the measures that meet the needs of the electronic payment institutions; also, ensure that the commissioned third party will, upon the request of the electronic payment institutions, provide the identity information or other relevant document photocopies needed for identifying the user without any delay.

III. Confirm that the commissioned third party is regulated, supervised, or monitored, and that appropriate measures are followed to ensure the identity of the user with the records kept.

IV. Confirm the location of the commissioned third party and the anti-money laundering and countering terrorism financing specifications is consistent with the standards enacted by The Financial Action Task Force on Money Laundering (FATF).

Article 8

Electronic payment institutions should have the name and title of the user checked in accordance with the following provisions:

I. The user's name and title check policies and procedures should be established in accordance with the risk-based approach in order to detect, compare, and screen whether or not the users, senior management of Category III electronic payment account non-personal

users, or real beneficiary of Category III electronic payment account non-personal user are the individuals, legal persons, or groups designated for sanctions by the Terrorism Financing Control Act, and the terrorists or terrorism groups identified or traced by foreign governments or international organizations.

II. For the confirmation methods stated in Item 1, Section 1, Article 4, the electronic payment institutions should check the data filled in the name column by the users at the time of establishing the business relationships. For any symbol, number, three-of-a-kind words, or special keywords identified, it is necessary to initiate identity verification check measure in order to prevent users from using a fake name.

III. The user's name and title check policies and procedures should at least include comparison and screening logic, the implementation procedures of checking operations, and the reviewing criteria in writing.

IV. The name and title check process shall be recorded and reserved in accordance with the deadline set out in Article 13.

This check mechanism should be tested and base on the test results to confirm whether the risk is still properly reflected and the check mechanism should be amended as appropriate.

Article 9

The continuous monitoring of accounts or transactions by the electronic payment institutions shall be handled in accordance with the following provisions:

I. Gradually integrate the basic information and transaction information of the users with the information system to conduct inquiries on the

prevention of money laundering and terrorism financing in order to strengthen their account or transaction monitoring ability. For each unit to retrieve and inquire about the user's data, establish an internal control procedure and pay attention to the importance of data confidentiality.

II. Base on the risk-based approach to establish the account or transaction monitoring policies and procedures; also, utilize an information system to assist in detecting suspected money laundering or terrorism financing transactions.

III. Base on the rules governing anti-money laundering and countering terrorism financing, the nature and business scale and complexity of users, the money laundering and terrorism financing related trend and information obtained internally and externally, and the internal risk assessment result of the electronic payment institutions to review the account or transaction monitoring policies and procedures that should be regularly updated.

IV. The account or transaction monitoring policies and procedures of the electronic payment institutions shall at least include the comprehensive monitoring patterns, parameter setting, threshold amount, operating procedures for early warning cases and monitoring operations, and the inspection procedures and reporting standards for the monitoring cases in writing.

V. Please refer to the annex for the complete monitoring patterns stated in the preceding section. The electronic payment institutions for the amount transfer of the electronic payment accounts should have all the information of the amount remitter and receiver included for the consideration of monitoring in order to determine whether or not to

report suspected money laundering or terrorism financing transactions.

VI. The electronic payment institutions shall report to the Investigation Bureau, Ministry of Justice the monitoring patterns prescribed in the preceding section or any other suspected money laundering or terrorism financing transactions for whatever an amount. Same for the transaction that is not completed.

VII. Electronic payment institutions shall, within 10 business days from the date of discovering and confirming the suspected money laundering or terrorism financing transactions, file an application with the Investigation Bureau, Ministry of Justice.

VIII. The continuing monitoring of an account or transaction shall be recorded and reserved in accordance with the deadlines set by the relevant laws and regulations.

Suspected money laundering or terrorism financing transaction declaration procedures:

I. The undertaker of each unit upon finding an abnormal transaction should report it immediately to the supervisor.

II. The supervisor should decide as soon as possible whether or not it is a reportable matter. If it is determined to be a reportable matter, the said undertaker should immediately fill out the reporting form (please have the form downloaded from the website of the Investigation Bureau, Ministry of Justice).

III. The reporting form should be submitted to the department head for approval and then forwarded to the responsible person.

IV. The reporting form after being forwarded to the functional head for approval by the responsible person should be reported to the Investigation Bureau, Ministry of Justice.

V. In the case of reporting a significant and urgent suspected money laundering or terrorism financing transaction, it shall be promptly reported to the Investigation Bureau, Ministry of Justice by fax or other feasible means with the written information submitted immediately thereafter. However, if the Investigation Bureau, Ministry of Justice confirms the recipient of the submission by fax (please have the form downloaded from the website of the Investigation Bureau, Ministry of Justice), there is no need to submit the written information. The electronic payment institutions shall keep on file the faxed recipient of the submission for records.

The requirements of confidentiality for preventing the disclosure of confidential data and information:

I. Personnel at all levels shall keep the reported matters as stated in the preceding paragraph in secret without committing any arbitrarily disclosure.

II. The documents related to this reporting matter should be handled in confident and any unauthorized disclosure should be handled in accordance with the relevant provisions.

III. The responsible persons and supervisors, compliance officers, or auditors for the need of performing job responsibilities may immediately access to user information and transaction records in compliance with the confidentiality requirements.

Article 10

For cooperation with overseas institutions or assisting foreign institutions to engage in the business operation of the electronic payment institutions in Taiwan, relevant policies and procedures should be enacted, including at

least:

I. Collect sufficient publicly available information in order to fully understand the business nature of the overseas institution and assess its goodwill and management quality, including compliance with the anti-money laundering and countering terrorism financing specifications.

II. Assess the overseas institutions' control policies and implementation effectiveness of anti-money laundering and countering terrorism financing.

III. The electronic payment institutions before cooperating with overseas institutions or assisting foreign institutions to engage in the business operation of the electronic payment institutions in Taiwan shall obtain the approval of the internal business supervisor in advance.

IV. Evidence the respective responsibilities for the anti-money laundering and countering terrorism financing with documents presented.

Article 11

Electronic payment institutions before launching new products or services or handling new types of business (including new delivery mechanisms and implementing new technologies onto the existing or new products or businesses) should evaluate the money laundering and terrorism financing risk exposure of the products and establish the corresponding risk management measures to reduce the identified risks.

Article 12

Currency transactions conducted for more than a certain amount of money should be handled in accordance with the following provisions:

I. Confirm the identity of the user with the relevant records and evidences

reserved.

II. Electronic payment institutions shall have the user identity confirmed in accordance with the following provisions:

(I) Confirm users' identity with the identity document or passport provided by the users; also, record their name, date of birth, telephone number, trading account number, transaction amount, and identity document number. However, if the user is confirmed as the principal of the trading account holder, the identity confirmation process is exempted. However, the fact that the transaction is completed by the principal should be stated in the transaction record.

(II) If the transaction is completed by an agent, the identity confirmation should be processed with the identity document or passport provided; also, the name, date of birth, telephone number, trading account number, transaction amount, and identity document number shall be recorded.

III. It shall be reported to the Investigation Bureau, Ministry of Justice within five business days after the completion of the transaction by means of media declaration (please have the form downloaded from the website of the Investigation Bureau, Ministry of Justice). Those who cannot complete the process by means of media declaration for a good reason may have it reported in writing (please have the form downloaded from the website of the Investigation Bureau, Ministry of Justice) with the consent of the Investigation Bureau, Ministry of Justice.

IV. The filing of documents to the Investigation Bureau and the reservation of the relevant records and evidences should be handled in

accordance with the provisions of Article 13.

Article 13

The electronic payment institutions shall keep the record of the transactions conducted with the users and the record of the transaction in writing or in an electronic form in accordance with the following provisions:

I. All necessary records of domestic and foreign transactions should be kept for a minimum of five (5) years. Unless otherwise provided by law for a longer period of time. The aforesaid necessary records shall be reserved in accordance with Article 21 of the "Regulations Governing Identity Verification Mechanism and Transaction Limits for Users of Electronic Payment Institutions."

II. The confirmed record and declared relevant record and evidence of a currency transaction up to a certain amount of money should be reserved in its original form for at least five (5) years. The electronic payment institution shall choose a recording method for the user confirmation procedures according to its own considerations and the principle of the company-wide consistency.

III. The relevant records and evidences of the suspected money laundering or terrorism financing transactions reported should be reserved in its original form for at least five (5) years.

IV. The following information shall be kept for at least five (5) years after the end of the electronic payment account or a currency transaction for a certain amount of money. Unless otherwise provided by law for a longer period of time:

(I) All records obtained for confirming user identity, such as, passport, identity card, driver's license, or similar official

identity documents photocopies or records.

(II) Electronic payment account file

(III) Business transaction information include the background or purpose information and data analysis obtained for inquiring the complicate and abnormal transactions.

V. The transaction records kept by the electronic payment institutions should be sufficient enough for reconstructing individual transaction for future reference in evidencing illegal activities.

VI. Electronic payment institutions should ensure that they are able to promptly provide transaction records and confirm the identity of the users upon the request of the authorized competent authorities.

Article 14

Functional head and responsible person:

I. The franchised electronic payment institutions shall allocate adequate personnel and resources for anti-money laundering and countering terrorism financing in accordance with its scale and risk; also, the Board of Directors (Executives) shall appoint one of the senior executives as the functional head to be in charge of coordinating and supervising the anti-money laundering and countering terrorism financing, and to ensure that such responsible persons and functional heads have no part-time job in conflict of interest with their responsibilities for anti-money laundering and countering terrorism financing.

II. The functional head in the preceding section is responsible for the following matters:

(I) Supervise the planning and implementation of the money

laundering and terrorism financing risk identification, assessment, and monitoring.

(II) Coordinate and supervise the implementation of comprehensive money laundering and terrorism financing risk identification and assessment.

(III) Monitor the risks associated with money laundering and terrorism financing.

(IV) Develop anti-money laundering and countering terrorism financing programs.

(V) Coordinate and supervise the implementation of anti- money laundering and countering terrorism financing programs.

(VI) Confirm the compliance with the anti-money laundering and countering terrorism financing relevant laws and regulations, including the relevant templates or self-regulatory specifications enacted by banker association and approved by the Financial Supervisory Commission for future reference.

(VII) Supervise the reporting of suspected money laundering and terrorism financing transactions to the Investigation Bureau, Ministry of Justice and the assets or property interests and the locations reported by the designated parties specified in the Terrorism Financing Control Act.

III. The functional head stated in Section 1 shall report to the Board of Directors (Executives) and the supervisors (supervisors, board of supervisors) or the Audit Committee at least once every six-month and report a material breach of the Act, if any, to the Board of Directors (Executive) and the Supervisors (supervisors, board of supervisors) or the Audit Committee.

IV. The overseas business units of the franchised electronic payment institutions shall set up adequate anti-money laundering and countering terrorism financing personnel based on the number of branches in the local area, business scale, and risks; also, they shall assign one (1) supervisor to be responsible for the coordination and supervision matters related to anti-money laundering and countering terrorism financing.

V. The appointment of the supervisors responsible for anti-money laundering and countering terrorism financing in the foreign business unit of the franchised electronic payment institutions should comply with the local laws and regulations and the requirements of the local authorities. They should also have the full authority to coordinate and supervise the anti-money laundering and countering terrorism financing, including reporting directly to the functional head as stated in Section 1; also, the supervisors should work full-time in addition to act as the Compliance Officer. If concurrently serving other duties, the supervisors should communicate with the local authorities to confirm that there is no risk of conflict of interest in their part-time employment and should report it to the Financial Supervisory Commission for future reference.

VI. The sideline electronic payment institutions should have the relevant requirements involving the functional head and responsible person handled in accordance with the relevant provisions of the industry.

Article 15

The implementation, auditing, and declaration of the anti-money laundering and countering terrorism financing internal control system:

I. The domestic and foreign business units of the franchised electronic payment institutions should appoint the senior management personnel as the supervisors to supervise their business units implementing the anti-money laundering and countering terrorism financing related matters, and handle the self-checking process in accordance with the "Rules Governing Internal Control and Audit System of Electronic Payment Institutions."

II. The internal auditing unit of the franchised electronic payment institutions should carry out the following auditing matters in accordance with the "Rules Governing Internal Control and Audit System of Electronic Payment Institutions" and with an audit opinion issued:

(I) Are the money laundering and terrorism financing risk assessment and anti-money laundering and countering terrorism financing program complied with the regulatory requirements and implemented comprehensively?

(II) Effectiveness of anti-money laundering and countering terrorism financing programs

III. Responsibilities of the internal auditing unit of an franchised electronic payment institution:

(I) Stipulate auditing matters in accordance with the internal control measures and the relevant provisions, implement auditing regularly, and test the effectiveness of anti-money laundering and countering terrorism financing programs and the risk management quality.

(II) The auditing method should include independent transaction tests, including screening of related transactions in respect of high-risk

products, users, and territories assessed by the electronic payment institutions and verifying the effective implementation of anti-money laundering and countering terrorism financing relevant specifications.

(III) The identified nonconformities of the said management measures should be regularly reported to the functional head for review and provided to the employees for reference in on-job training.

(IV) The intentional concealment of major nonconformities shall be properly handled by the responsible unit in the head office.

IV. The general manager of the franchised electronic payments institution shall supervise each unit to evaluate and review prudently the implementation of the internal control system for anti-money laundering and countering terrorism financing. The statement of internal control system for anti-money laundering and countering terrorism financing should be issued jointly by the Chairman (Executive), the general manager, the auditor, the functional head for anti-money laundering and countering terrorism financing. Also, the said statement should be reported to the Board of Directors (Executives) for approval. The statement of internal control system should be disclosed within three (3) months after the end of each fiscal year on the electronic payment institution's website and on the website designated by the Financial Supervisory Commission.

V. The sideline electronic payment institutions should have the implementation of the internal control system, audit, and declaration related requirements handled in accordance with the relevant provisions of the industry.

Article 16

Employee appointment and training:

I. The franchised electronic payment institutions should establish a prudent and appropriate staff recruitment and appointment procedure that includes checking the integrity of employees and the professional knowledge needed to perform their duties.

II. The functional head, responsible person, and the supervisor of the domestic business unit of the franchised electronic payment institutions must meet one of the following eligibility criteria within three (3) months after assuming the job responsibility. The electronic payment institutions shall also set the relevant control mechanism to ensure their complying with the requirements:

(I) Served full-time as a compliance officer or a responsible person for anti-money laundering or countering terrorism financing for more than three (3) years.

(II) Participated in the courses arranged by the institutions authorized by the Financial Supervisory Commission for more than 24 hours and passed the examination with a certificate of completion obtained. Those who have been qualified as a compliance officer, after participating in the 12-hour anti-money laundering and countering terrorism financing courses arranged by the institutions authorized by the Financial Supervisory Commission, are deemed as meeting the eligibility criteria illustrated in this Item.

(III) Received a certificate of qualification after attending the domestic or international anti-money laundering and countering terrorism financing courses arranged by the institutions authorized by the Financial Supervisory Commission.

III. Persons in the preceding section who were appointed before June 30, 2017will be deemed eligible upon meeting one of the following conditions:

(I) Meet the eligibility criteria stated in Item 1 or Item 3 of the preceding section before June 30, 2017.

(II) Meet the eligibility criteria stated in Item 2 of the preceding section within the following period of time:

1. For the functional head and responsible person of the electronic payment institutions in charge of anti-money laundering and countering terrorism financing, the deadline is before December 31, 2017.
2. For the domestic business unit supervisors of the electronic payment institutions, the deadline is within one (1) year after assuming the position.

IV. The functional head and responsible person in charge of anti-money laundering and countering terrorism and the domestic business unit supervisor of the franchised electronic payment institutions shall at least participate in the 12-hour anti-money laundering and countering terrorism financing courses arranged by the internal or external training units authorized by the functional head as stated in Section 1, Article 14. The training program should include at least the newly amended ordinances and the money laundering and terrorism financing trends and patterns. Those who have received a certificate of qualification after attending the domestic or international anti-money laundering and countering terrorism financing courses arranged by the institutions authorized by the Financial Supervisory Commission may be applied as credit hours waiver.

V. The foreign business units supervisors and anti-money laundering and countering terrorism financing supervisor and personnel of the franchised electronic payment institutions shall have anti-money laundering professional knowledge and be familiar with local laws and regulations; also, they shall attend at least 12-hour anti-money laundering and countering terrorism financing courses arranged by foreign competent authorities or relevant agencies annually. If foreign authorities or related organizations do not hold any anti-money laundering and countering terrorism financing education and training courses, they may participate in the courses arranged by the internal or external training units authorized by the functional head as stated in Section 1, Article 14.

VI. The directors (executives), supervisors, general manager, compliance officer, internal auditors, and salespersons of the franchised electronic payment institutions shall, according to the nature of their businesses, arrange anti-money laundering and countering terrorism financing education and training courses with appropriate content and time annually to help them understand their responsibilities for anti-money laundering and countering terrorism financing; also, to help them acquire the needed professions for job performance.

The job performance of employees should be randomly inspected in any of the following circumstances with the assistance of the audit unit, if necessary:

I. The extravagant life style of employees is not comparable with their salary income.

II. Staff has failed to take the scheduled leave without any reason.

III. Employees cannot reasonably explain the large amount of capital in

and out of their own accounts.

Employees who have the following specific achievements in anti-money laundering or countering terrorism financing should be awarded accordingly:

I. Employees reported suspicious money laundering or terrorism financing cases in accordance with the relevant provisions of anti-money laundering and helped the law enforcement agency prevent or detect crimes successfully.

II. Employees participated in domestic and international anti-money laundering or countering terrorism financing related seminars with good grades obtained, or collected information on foreign laws and regulations to study and propose valuable data on anti-money laundering or countering terrorism financing.

Pre-employment and on-job training should be handled in the following manners:

I. Pre-employment Training: New Staff Training should be arranged with at least certain hours of anti-money laundering and countering terrorism financing law and regulations, and financial practitioners legal responsibilities training courses to help new employees understand the relevant regulations and responsibilities.

II. On-job training:

(I) Preliminary decrees propaganda: After the implementation or amendment of the Money Laundering Control Act and the Terrorism Financing Control Act, the decrees should be advertised to the employees over the shortest period of time, the Money Laundering Control Act, Terrorism Financing Control Act, and the relevant laws and regulations should be introduced,

and the relevant responsive measures of the electronic payment institutions should be explained. The relevant matters planned by the functional head should be implemented by the staff training unit.

(II) Regular on-job training:

1. The staff training department shall regularly organize relevant training courses for the study of the staff every year in order to enhance the staff's judgment, substantiate the anti-money laundering and countering terrorism financing functions, and prevent staff from breaking the law. The related courses of this training can be arranged in other specialized training programs.
2. The training courses shall be lectured by the instructors of the electronic payment institutions and the academics or experts contracted, if necessary.
3. Apart from introducing relevant laws and regulations, the training course should be supplemented with case studies so that staff can fully understand the characteristics and types of money laundering and terrorism financing in order to help them detect "suspected money laundering or terrorism financing transactions."
4. The functional head should regularly understand the employees' participation in the training. For those who have not participated in the training, the functional head should urge them to participate in the relevant training according to actual needs.
5. In addition to the internal on-job training, the electronic payment institutions should also send their staff to take training courses organized by external training institutions.

III. Keynote Speech: In order to make employees more aware of the Money Laundering Control Act and the Terrorism Financing Control Act, the electronic payment institutions may hold a keynote speech seminar and invite experts and scholars to give lectures.

IV. The sideline electronic payment institutions should have the staff appointments and training related provisions handled in accordance with the relevant provisions of the industry.

Article 17

Other guidelines:

I. The users will be declined of service in the following situations and it should be reported to the direct supervisor:

(I) The users refuse to provide the relevant information for identity confirmation upon a lawful request.

(II) The users force or attempt to force the employees of the electronic payment institutions not to file a transaction record or declaration form.

(III) The users intend to persuade the employees of the electronic payment institutions not to complete the reporting data of a transaction.

(IV) Try to avoid the obligation of reporting.

(V) The user's description does not match the transaction took place.

(VI) The users attempt to offer benefits to employees in exchange for receiving services from the electronic payment institutions.

II. When the franchised electronic payment institutions operate other businesses concurrently, the sideline business is also subject to the "Guidelines for Anti-Money Laundering and Countering Terrorism

Financing for Electronic Payment Institutions (Template)"that is related to the business operation, for example, if the electronic payment institutions operate concurrently the electronic stored value card business, the electronic stored value card business is subject to the provisions of the "Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Electronic Payment Institutions (Template)."

Article 18

The electronic payment institutions shall refer to the "Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Electronic Payment Institutions (Template)" for the stipulation of other guidelines, which should be implemented with the approval of the Board of Directors (Executives) and reported to the Financial Supervisory Commission for future reference and should be reviewed annually. Same for the amendments

Article 19

The Template shall be resolved in the executive meeting of the Association and reported to the Financial Supervisory Commission for future reference, same for the amendments.