The Bankers Association of the Republic of China
"Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Electronic Stored Value Card Issuers (Template)."

Financial Supervisory Commission on December 24, 2015
FSC.Banking.Bills.Tzi No. 10400281060 Letter approved for future reference
Financial Supervisory Commission on September 30, 2017
FSC.Banking.Bills.Tzi No. 10600225180 Letter approved for future reference

Article 1

The "Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Electronic Stored Value Card Issuers (Template)" is enacted in accordance with the "Money Laundering Control Act,""Terrorism Financing Control Act," "Regulations Governing Anti-Money Laundering of Financial Institutions,""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," and "Rules Governing the Business of Electronic Stored Value Card Issuers."

Article 2

The internal control system established by the electronic stored value card issuers shall be approved by the Board of Directors (Executives), same for the amendment. 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 Stored Value Card Issuers" (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 Stored Value Card Issuers," 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 customer, 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 customer identity;

II. Checking the name and title of the customers and the transaction related parties

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.

The electronic stored value card issuers 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 customer 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 customers, 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 stored value card issuers 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 the subsidiary company) 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 stored value card issuers 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.

The Board of Directors (Executives) of the electronic stored value card issuers 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) A certain quantity: Fifty electronic stored value cards

(III) Currency transactions: It refers to one single transaction of cash received or paid, including the purchase of electronic stored value card, stored value, redemption, and return (it refers to all cash receipt and payment vouchers in accounting process).

(IV) Electronic stored value card: It refers to the stored value in an electronic, magnetic, or optical form, including data storage or calculation chip and card, voucher, or other form of debt as a multi-purpose payment mean.

(V) Electronic stored value card issuers: It refers to the electronic stored value card issuers authorized in accordance with the Act Governing Issuance of Electronic Stored Value Cards.

(VI) Customer: It refers to the cardholders of the electronic stored value card issuers or the persons who have the interim transactions conducted over the counter.

(VII) Registered electronic stored value card: It is limited to the use of the registered cardholder who is entitled to the service of loss and found for the electronic stored value card.

(VIII) 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.

(IX) Establishment of a business relationship: It refers to the electronic stored value card registration process arranged for customers by the electronic stored value card issuers.

(X) Interim transactions: It refers to not establishing a business relationship with the electronic stored value card issuers but conducting a currency transaction for a certain amount of money or a number of electronic stored value card transactions, several significantly connected currency transactions for a certain amount of money.

(XI) Risk-based approach: An electronic stored value card issuer 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 stored value card issuer 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

Confirmation of customer's identity shall be handled in accordance with the following:

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

(I) Suspected of arranging electronic stored value card registration operation by an anonymous, pseudonym, head, dummy company, or dummy legal person group.

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

(III) In the case of an electronic stored value card registration operation or transaction handled by an agent with difficulty in verifying the fact of the agency and the identity of the agent;

(IV) Use of false or altered identity documents.

(V) Proof of identity documents presented as photocopies. 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) Suspicious or obscure documents provided, and unwillingness to

provide other supporting data or the provided data is unable to be verified.

(VII) Supplementary customer identity documents are provided after an unreasonable delay.

(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) When establishing a business relationship or conducting a business transaction with other abnormalities that the customers are unable to give reasonable explanations.

II. The timing of confirming customer's identity:

(I) When establishing a business relationship with a customer

(II) Make an interim transaction.

(III) Discover suspected money laundering or terrorism financing transactions.

(IV) When the authenticity or appropriateness of the customer's identity information is in doubt.

III. Confirmation of customer's identity shall be handled in accordance with the following:

(I) The identity of the customer should be identified and verified according to the dependable and independent source of documents, data, or information and with the photocopy of the identity document or record kept.

(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) The real beneficiary of the customer must be confirmed and its identity is to be verified with reasonable measures, including the use of reliable sources of data or information. However, the electronic stored value card registration operation is not subject to the provision of this item.

(IV) Confirmation of customer identity measures should include understanding the purpose and nature of the business relationship and obtaining information as appropriate.

IV. Customers 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 stored value card issuers, at least one of the following information should be obtained when establishing a business relationship:

(I) The name or alias used: The name used previously, such as, the name used before getting married or the name used before a name change.

(II) Office address, PO Box address, e-mail address (if any)

(III) Phone or cell phone number.

V. According to the provision of Section 3, when the customer is entrusted by a legal person, group, or trust, it is necessary to understand the business nature of the customer or trust (including a legal agreement similar to the trust) and obtain at least the following information from the customer or trust to identify and verify the customer identity:

(I) The name, legal for, and proof of existence of the customer or trust.

(II) Regulate and manage the articles of association or similar authority document of the legal person, group, or trust. However, it is not applicable in the following circumstances:

1. The objects stated in Item 3, Section 7 are without the proviso stated in Section, 3, Paragraph 1, Article 6.

2. Salespersons for electronic stored value card registration operation

3. Group customers who are confirmed without the association or similar authority document enacted.

(III) Name of the senior management who are entrusted by a legal person, group, or trust

(IV) The registered office address of the individuals entrusted by a legal person, group, or trust and the principal place of business

VI. According to the provision of Item 3, Section 3, when the customer is entrusted by a legal person, group, or trust, it is necessary to understand the ownership and control structure of the customer or trust; also, identify the real beneficiary of the customer through the following information and take reasonable measures to verify:

(I) When the customer is a legal person or a group:

1. The identity (e.g. Name, date of birth, nationality, identity card number, etc.) of the controlling ultimate natural person The term "control" means directly or indirectly holding more than 25% of the shares or capital of the legal person, and the electronic stored value card issuers may require the customer to provide the register of shareholders or other documents to assist in the identification.
2. According to the provision of the preceding Sub-item, 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 customer through other means. If necessary, obtain a statement from the customer to confirm the identity of the real beneficiary.
3. In the absence of any foreseeable natural person identified as stated in the last two Sub-items, the electronic stored value card issuers should identify the identity of the senior management.

(II) When the customer is entrusted by a trust: It is necessary to identify the identity of the principal, the entrusted person, the trust supervisor,

the beneficiary of the trust, and others who have effective control of the trust account, or persons who have similar or equivalent responsibilities as the aforementioned personnel.

(III) Customer or controlling persons with any of the following identities, except for the proviso stated in Section, 3, Paragraph 1, Article 6 or with bearer stock shares issued, are not subject to the aforementioned requirements of identifying and confirming the identity of the real beneficiary as stated in Item 3, Section 3:

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 stored value card issuers 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.
8. The funds managed by the government agencies of Taiwan
9. Employee Shareholding Trust and Employee Benefits Savings Trust

VII. Customer 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 stored value card issuers should be verified with more stringent measures adopted, such as:

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

(II) Obtain supporting document on personal wealth and fund sources information.

(III) 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 customers, etc.

(IV) Field visits

(V) Obtain previous bank contact information with the said bank notified.

VIII. The electronic stored value card issuers shall not establish business relationship with the customers or make any interim transactions until their have completed the process of confirming customer identity. However, those who meet the following conditions must first obtain the information for identifying the identity of customers and real beneficiaries with the verification completed after the business relationship established:

(I) Money laundering and the terrorism financing risks are effectively managed. It includes the risk control measures adopted for the possibility of identity verification not completed by the customers until the transactions are completed.

(II) It is necessary to prevent interfering with the normal business operation of the customers.

(III) Verify the identity of the customer and real beneficiary under a reasonable and practicable circumstance. If the identity of the customer and the real beneficiary is not verified within the reasonable

time frame, the business relationship should be ended with the customers informed in advance.

IX. If the electronic stored value card issuers allow customers to establish a business relationship before completing identity verification, the relevant risk control measures shall be taken, including:

(I) Set customer identity verification deadline.

(II) Prior to the completion of customer identity verification, the supervisor of the business unit should periodically review the current relationship with the customer and regularly report the progress of the customer identity verification process to the management.

(III) For the "within the reasonable time frame" stated in Item 3 of the preceding section, the electronic stored value card issuers should base on the risk-based approach to stipulate the risk levels accordingly.

X. When the customer is a legal person, understand whether there is bearer stock shares issued by examining the articles of association or asking the customer to issue a statement; also, take one of the following measures against the customer who has issued bearer stock shares to ensure the updating of the real beneficiaries. However, the issuance of order stock is not subject to this provision:

(I) The customers should request the controlling shareholders with bearer stock shares to have the customers informed for identity registration; also, the customers should have the electronic stored value card issuers informed when there are changes in the identity of the controlling shareholders.

(II) The customers should update the information of the real beneficiary with the electronic stored value card issuers after each shareholder's meeting; also, provide the information of shareholders holding a certain percentage of the bearer stock shares. However, the customer shall notify the electronic stored value card issuers immediately when

it becomes aware of any change in the status of the controlling shareholder for any reason.

XI. Electronic stored value card issuers upon confirming the identity of the customer should make use of the self-constructed database or external information sources to check whether the customers and their real beneficiaries and senior management are or were politically exposed persons of Taiwan, foreign governments, or international organizations.

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

(II) If the customers or their real beneficiaries are currently a politically exposed person of the domestic government or an international organization, the related risks shall be reviewed at the time of establishing a business relationship with the customers and they shall be reviewed again annually. Customers identified as with high-risk by electronic stored value card issuers 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 customer is a politically exposed person of Taiwan, a foreign government, or an international organization, the electronic stored value card issuers shall consider the influence of the senior manager on the customer and decide whether the customer 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 stored value card issuers 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 (3) items.

(V) The provisions of the last four (4) 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) When the customer is the government agency of Taiwan, the state-run business institution, a foreign government agency, or a fund managed by the government agency of Taiwan, the real beneficiary or senior management of the customer that is a politically exposed person is not subject to the provision of Item 1 – Item 5 of this Section.

XII. Confirmation of customer's identity and other compliance related matters:

(I) Electronic stored value card issuers should confirm and record the customers' identity according to the government-issued or other identification documents when establishing business relationships with the customers, when the financial transactions conducted with the interim customers exceeding a certain amount, or when the customers' information is not sufficient enough to confirm their identity.

(II) For "non-face-to-face" customers or online business associates, a customer validation procedure with the same effect should be applied and special and adequate measures must be taken to mitigate the risk.

(III) For the customers 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) Without prejudice to the relevant laws and regulations, electronic stored value card issuers should not accept or should cut off business relationships if they know or must assume that customers' funds come

from corruption or abuse of public assets.

(V) Electronic stored value card issuers should consider reporting any suspicious money laundering or terrorism financing transactions of the customers if they failed to complete the relevant procedures of identity confirmation.

(VI) If an electronic stored value card issuer suspects that a customer or transaction may involve money laundering or terrorism financing, and reasonably believes that performing identity confirmation procedure may reveal such information to the customer, the electronic stored value card issuer may report a suspected money laundering or terrorism financing transaction instead of performing the said procedure.

(VII) Other matters needing attention while establishing a business relationship should be handled in accordance with the internal operating requirements of the electronic stored value card issuer.

XIII. 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 stored value card issuer may turn down a business transaction or may have a business relationship terminated.

(II) For those who do not cooperate with the review, refuse to provide information on the real beneficiaries or the individuals who exercise power over the customers, or refuse to explain the nature and purpose of the transaction or the source of funds, the electronic stored value card issuers may have the transactions ceased or suspended temporarily according to the agreement, or have the use of the electronic stored value card terminated.

XIV. Where a business relationship or trade counterparty is established as described in Item 8, Section 1, electronic stored value card issuers 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 stored value card issuers 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 stored value card issuers 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 stored value card issuers for confirming customer identity should include the ongoing due diligence for customer identity and it should be handled in accordance with the following provisions:

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

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

according to the risk-based approach.

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

Article 6

The level of due diligence for the customer identity confirmation measures and ongoing due diligence stated in Section 3, Article 4, and the preceding Article should be determined in accordance with the risk-based approach by the electronic stored value card issuers, including:

I. Implement enhanced due diligence or ongoing due diligence for customers 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 stored value card issuers shall obtain the approval of the senior management. However, the electronic stored value card registration operation is not subject to the provision of this item.

(II) Adopt reasonable measures to understand the wealth of the customers and the source of funds. The source of funds refers to the real source of the funds. However, the electronic stored value card registration operation is not subject to the provision of this item.

(III) The business relationship shall be supervised forcefully and

continuously.

II. Adopt enhanced measures commensurate with the risk for the customers from 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 their lower risk factors. However, simplified measures shall not be adopted for the confirmation of customer identity in the following circumstances:

(I) For customers 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 include but not limited to the countries or regions with serious nonconformities 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, and other countries and regions that failed to comply or fully comply with the advice of the International Anti-Money Laundering Organizations.

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

Electronic stored value card issuers should review the existing customers in accordance with the importance and degree of risk. After considering the timing of the last customer review and the adequacy of the information obtained, the electronic stored value card issuers shall review the existing relationships at an appropriate time.

Article 7

Electronic stored value card issuer should handle the customer identity confirmation on its own initiative. If it is otherwise provided by law or the competent authority that the electronic stored value card issuer may rely on the

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

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

II. Adopt the measures that meet the needs of the electronic stored value card issuer; also, ensure that the commissioned third party will, upon the request of the electronic stored value card issuer, provide the identity information or other relevant document photocopies needed for identifying the customer 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 customer with the records kept.

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

Article 8

Electronic stored value card issuers should have the name and title of the customer and trade counterparty checked in accordance with the following provisions:

I. The customer's and trade counterparty'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 customers, senior management, real beneficiary, or trade counterparties of the customers 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. If so, it shall be processed in accordance with the provisions of Section 14, Article 4.

II. The customer's and trade counterparty'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.

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

IV. 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 stored value card issuers shall be handled in accordance with the following provisions:

I. Gradually integrate the basic information and transaction information of the customers with the information system for the company (branch) to conduct inquiries on the prevention of money laundering and terrorism financing in order to strengthen its account or transaction monitoring ability. Establish internal control procedures for the data retrieval and customer information query of each department, and pay attention to the confidentiality of information.

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 customers, the money laundering and terrorism financing related trend and information obtained internally and externally, and the internal risk assessment result of the financial 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 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. When the electronic stored value card issuers discover or have reasonable grounds to suspect that the customers, customers' funds, assets or the intended/executed transactions involving money laundering or terrorism financing, the identity of the customers shall be reviewed further regardless the amount or value of the transaction or the completion or not of the transaction.

VI. The signs of the transactions suspected of money laundering or terrorism financing are illustrated in the annex, but it is not exhaustive. The electronic stored value card issuer should base on its own asset scale, geographical distribution, business features, customer nature, and transaction characteristics, and refer to the internal money laundering and terrorism financing risk assessment or daily trading information to select or develop its own warning signs in order to identify the cautionary transactions suspected of money laundering or terrorism financing.

VII. The cautionary transactions identified in the preceding paragraph should be judged on the merits of each individual case (the judgment of reasonableness, for example, whether it is inconsistent with the identity of the customer, the scale of revenue, or business scale; whether it is irrelevant

to the business nature of the customer, the business model of the customer, it is without reasonable economic purposes, no reasonable explanation, no reasonable use, or unclear sources of funds or accountability) with the saved inspection records. If it is determined that there is no suspicion of money laundering or terrorism financing, the reason for such conclusion should be recorded. If it is determined that there is suspicion of money laundering or terrorism financing, in addition to confirming the identity of the customer and keeping the relevant records, the transaction suspected of money laundering or terrorism financing should be reported to the Investigation Bureau, Ministry of Justice within 10 business days from the day it is discovered and identified within the electronic stored value card issuers.

VIII. Electronic stored value card issuers shall base on the risk-based approach to have the relevant information systems established in order to assist in the monitoring of the suspected money laundering or terrorism financing. For those not included in the system for monitoring, the electronic stored value card issuers should help employees determine whether the transaction is suspected of money laundering or terrorism financing with other means. The system assistance does not completely replace the staff's judgment. Therefore, the electronic stored value card issuers should still strengthen the staff training to help employees identify transactions suspected of money laundering or terrorism financing.

Electronic stored value card issuers should have the declaration of the suspected money laundering or terrorism financing handled in accordance with the following provisions:

I. The transactions suspected of money laundering or terrorism financing should be filed with the functional head for approval in 10 business days upon discovery in the reporting format specified by the Investigation Bureau and it should also be reported to the Investigation Bureau thereafter.

II. 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, there is no need to submit the written information. The electronic stored value card issuers shall keep on file the faxed recipient of the submission for records.

III. The declaration forms and fax confirmation slip stated in the last two sections should be handled in accordance with the format of the Investigation Bureau.

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.

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 for anti-money laundering, compliance officers, or auditors for the need of performing job responsibilities may immediately access to customer’s information and transaction records in compliance with the confidentiality requirements.

Electronic stored value card issuers should have the continuous monitoring of the account or transaction recorded and reserved in accordance with the deadline set out in Article 13.

Article 10

For the issuance of international electronic stored value card or for the cooperation with overseas institutions to engage in the business operation of the electronic stored value card issuers, the electronic stored value card issuers should have the relevant policies and procedures 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. For the issuance of international electronic stored value card or for the cooperation with overseas institutions to engage in the business operation of the electronic stored value card issuers, the electronic stored value card issuers should 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 stored value card issuers 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

Electronic stored value card issuers should have the currency transactions for a

certain amount of money handled in accordance with the following provisions

I. Confirm the identity of the customer with the relevant records and evidences reserved.

II. Confirm the customer identity in accordance with the following provisions:

(I) Confirm customers' identity with the identity document or passport provided by the customers; also, record their name, date of birth, address, telephone number, trading account number, transaction amount, and identity document number. If the customer can be verified as the principal, it is not necessary to initiate the identity confirmation process; however, it shall be indicated as a transaction completed by the principal in the transaction records.

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

(III) For an interim transaction, the identity of the customer shall be confirmed in accordance with the provisions of Section 3, Article 4.

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.

Electronic stored value card issuer is exempted from reporting to the Investigation Bureau, Ministry of Justice the currency transaction conducted with financial institutions for a certain amount of money as stated in Paragraph 1, Article 14 of the Money Laundering Control Act, but shall still confirm the identity of the customer and keep the relevant records and document. The transaction suspected of money laundering or terrorism financing identified should be handled in accordance with Article 10 of the Money Laundering Control Act and Paragraph 2, Article 7 of the Terrorism Financing Control Act.

Article 13

The electronic stored value card issuers shall keep the record of the transactions conducted with the customers 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 necessary records in the preceding paragraph include:
   (I) Account or card number of each party involving in the transactions
   (II) transaction date
   (III) Trading items
   (IV) Type of transaction currency and amounts
   (V) Trading equipment code
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.
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

conclusion of the business relationship with the customer or after the conclusion of the interim transaction. Unless otherwise provided by law for a longer period of time:

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

(II) Electronic stored value card account files

(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 should be sufficient enough for reconstructing individual transaction for future reference in evidencing illegal activities.

VI. Electronic stored value card issuers 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 electronic stored value card issuers 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 (1) of the senior executives as the functional head to be in charge of coordinating and supervising the anti-money laundering and countering terrorism financing. 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 policies and procedures for money laundering and terrorism financing risk identification, assessment, and monitoring.

(II) Coordinate and supervise the implementation of the 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 the 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 electronic stored value card issuers 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, shall assign one 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 electronic stored value card issuers 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.

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 electronic stored value card issuers 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.

II. The internal auditing unit of the electronic stored value card issuers should carry out the following auditing matters in accordance with the regulations and with an audit opinion issued:

(I) Are the money laundering and terrorism financing risk assessment and

the anti-money laundering and countering terrorism financing programs in compliance with the regulatory requirements and properly implemented?

(II) The effectiveness of the anti-money laundering and the countering terrorism financing programs

III. Responsibilities of the internal auditing unit of the electronic stored value card issuers:

(I) The auditing process should be enacted in accordance with the internal control measures and the relevant provisions. The audit should be conducted on a regular basis; also, the effectiveness of the anti-money laundering and countering terrorism financing program and the risk management quality of the operation departments and branches of the electronic stored value card issuers should be tested.

(II) The auditing method should include independent transaction tests, including screening of related transactions in respect of high-risk products, customers, and territories assessed by the electronic stored value card issuers, 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 electronic stored value card issuers 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 chief 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 stored value card issuers' website and on the website designated by the Financial Supervisory Commission.

Article 16

Employee appointment and training:

I. The electronic stored value card issuers 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 electronic stored value card issuers must meet one of the following eligibility criteria within three (3) months after assuming the job responsibility.The electronic stored value card issuers shall also set the relevant control mechanism to ensure their complying with the requirements:

(I) Those who have served as a compliance officer or have been responsible for anti-money laundering and 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) 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

III. The personnel stated in the preceding paragraph who have reported to duty before June 30, 2017 shall be deemed as in compliance with the eligibility criteria after meeting one of the following conditions:

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

(II) Meet the eligibility criteria as stated in Item 2 in the preceding section before deadline as follows:

1. For the functional head and responsible person in charge of anti-money laundering and countering terrorism financing, the deadline is before December 31, 2017.
2. For the domestic business unit supervisors, the deadline is within one 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 electronic stored value card issuers 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 electronic stored value card issuers shall have anti-money laundering professional knowledge and be familiar with local laws and regulations; also, 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 electronic stored value card issuers 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.

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 to the electronic stored value card issuers.

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 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 stored value card issuers should be explained. The relevant matters planned by the unit responsible for anti-money operation 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 stored value card issuers 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 stored value card issuers 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 stored value card issuers may hold a keynote speech seminar and invite experts and scholars to give lectures.

Article 17

Other guidelines:

I. The customers 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 customers force or attempt to force the employees 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) Eager to explain the source of funds is innocent or non-money-laundering related.

(VI) Insist on having the transaction completed immediately, without giving a reasonable explanation.

(VII) The customer's description does not match the transaction took place.

(VIII) The customers attempt to offer benefits to employees in exchange for receiving services from the electronic stored value card issuers.

II. When the electronic stored value card issuers operate other businesses concurrently, the sideline business is also subject to the "Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Electronic Stored Value Card Issuers (Template)" that is related to the business operation, for example, if the electronic stored value card issuers operate concurrently the electronic stored value card business, the electronic stored value card issuers are subject to the provisions of the "Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Electronic Stored Value Card Issuers (Template)."

Article 18

The electronic stored value card issuers shall refer to the "Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Electronic Stored Value Card Issuers (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.

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.