

# **“Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control Programs by Electronic Stored Value Card Issuers”**

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

- I. The “Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control Programs by Electronic Stored Value Card Issuers” is enacted in accordance with the “Directions Governing Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business, Electronic Payments Institution, and Electronic Stored Value Card Issuers” for the purpose of anti-money laundering and countering terrorism financing. It covers the subjects of “how electronic stored value card issuers recognize and assess the money laundering and terrorism financing risks” and with the anti-money laundering and countering terrorism financing programs enacted for reference in implementation.
  
- II. The internal control system of an electronic stored value card issuer shall be approved by the Board of Directors (Executives), same for the amendment. Its contents should include the identification, assessment, and management of the money laundering and terrorism financing risks, the stipulation of the related written policies and procedures, the anti-money laundering and countering terrorism financing program formulated in accordance with the risk assessment result, and a regular review.

A risk-based approach is designed to assist in the development of a control and counter measure that is commensurate with the money laundering and terrorism financing risk in order to help electronic stored value card issuers determine the allocation of anti-money laundering and countering terrorism financing

resources, establish an internal control system, and stipulate and implement the policies, procedures, and control measures of an anti-money laundering and countering terrorism financing program.

The instructions cited in the “Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control Programs by Electronic Stored Value Card Issuers” are not mandatory norms. The risk assessment mechanism of the electronic stored value card issuers should be commensurate with the nature and size of the business operations. For smaller or simpler electronic stored value card issuers, a simple risk assessment is sufficient; however, for electronic stored value card issuers with complex products and services and with a wide range of products provided by multiple branches or with the products and services used by diversified customers, a higher degree of risk assessment procedure should be performed.

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

The specific risk assessment items should include at least the geography, customers, products and services, transaction or payment pipeline, etc., and should further analyze each risk item to stipulate detailed risk factors.

(I) Regional risk:

1. Electronic stored value card issuers should identify the areas at higher risk of money laundering and terrorism financing.
2. In setting a list of regions with high risk of money laundering and terrorism financing, electronic stored value card issuers may choose the applicable reference criteria based on the actual experience of their respective branches and taking into account the individual needs.

(II) Customer risk:

Electronic stored value card issuers should base on the following risk factors to consider the money laundering and terrorism financing risks of each customer.

- (1) Geographical risk of customers: Base on the list of areas with the risk of money laundering and terrorism financing defined by the electronic stored value card issuers to determine the customer's nationality and country of residence risk.
- (2) Occupation and industry money laundering risk of customers: Base on the money laundering risk of each occupation and industry defined by the electronic stored value card issues to determine the customer's occupation and industry risk. High-risk industries refer to the companies or trusts engaged in cash-intensive business transaction or those easily being used to hold personal assets.
- (3) The quantity of electronic stored value cards purchased by the customers and the channel of purchase
- (4) The amount of the stored value purchased by the customer and the channel of purchase
- (5) The amount of stored value redeemed or refunded by the customer, and the channel of purchase
- (6) The registration channel of customers
- (7) Electronic stored value card transaction amount of the customers
- (8) Whether the customers are with other signs of high money laundering and terrorism financing risks, such as, the customer is a foreigner without a residence permit or non-resident national who does not hold a residence registration and cannot give reasonable explanations; the customer is a company and an anonymous shareholder or a company that can issue bearer stock. The complexity of the shareholdings of corporate customers, such as, the obvious abnormality of the shareholding structure or the high

complicity of the shareholding structure comparing to its business nature.

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

1. Electronic stored value card issuers should base on the nature of each product and service, trading, or payment pipeline to identify those with high risk of money laundering and terrorism financing.
2. 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.
3. Individual product and service, trading, or payment pipeline risk is illustrated as follows:
  - (1) It is not easy to trace the source of funds or difficult to identify identity.
  - (2) Cash out operation.
  - (3) Is it a large amount or high value transfer operation?
  - (4) Anonymous trading.
  - (5) Received money from unknown or unrelated third parties.

IV. Electronic stored value card issuers should establish different customer risk levels and classification rules.

The risk of the customer shall include at least two or more risk levels, namely, “high risk” and “general risk,” as the basis for enhanced due diligence and intensive and continuous monitoring mechanism.

For electronic stored value card issuers with only a two-level risk rating, the “general risk” rating is higher than the “low-risk” rating as indicated in Points 5 and 7 of the “Guidance on Assessment of Money Laundering and Terrorism

Financing Risks and Formulation of Related Control Programs by Electronic Stored Value Card Issuers;” therefore, a simple measure is not applicable to the customer with “general risk.”

Electronic stored value card issuers shall not disclose the customer’s risk level information to the customer or other persons who are not involved in the implementation of anti-money laundering or countering terrorism financing obligations.

- V. Except for the politically exposed persons of a foreign government and those who faced economic sanctions, terrorists or terrorism group charged or traced by foreign governments or by the International Money Laundering Prevention Organization, and the individuals, legal persons, or groups designated by the Terrorism Financing Control Act for sanctions shall be directly considered as high-risk customers, the electronic stored value card issuers should set the types that should be directly considered as high-risk customers according to their business models and considering the relevant risk factors.

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

- VI. For newly registered customers, the electronic stored value card issuers shall determine their risk level while establishing the business relationship.

For existing customers with a defined level of risk, the electronic stored value card issuers should re-perform the customer risk assessment in accordance with its risk assessment policies and procedures.

Although the electronic stored value card issuers have conducted risk assessments on customers when establishing the business relationship, for

certain customers, the overall risk profile of the customers will not be clarified until the customers make transactions through an account. Thus, the electronic stored value card issuers should review the identity data of 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 and adjust the customer's risk level accordingly. The aforementioned appropriate timing shall include at least:

- (I) The electronic stored value card issuers according to obvious evidence believe that it is necessary to confirm the identity of the customer again.
- (II) Periodic reviews are determined in accordance with the importance and risk level of the customer.
- (III) When there are important changes to the customer's identity and background information.
- (IV) When reporting a suspected money laundering or terrorism financing transaction, an event that may lead to a material change in the customer's risk profile occurs.

Electronic stored value card issuers should 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, electronic stored value card issuers should have them reviewed at least once a year.

VII. Electronic stored value card issuers should establish corresponding control measures based on the identified risks in order to reduce or prevent the money laundering risks. Electronic stored value card issuers shall determine the respective control measures applicable to customers with different risk levels accordingly.

For the risk control measures, electronic stored value card issuers should adopt

different control measures based on their risk control policies and procedures for different types of high-risk customers and those with specific high-risk factors in order to effectively manage and reduce the known risks as follows:

- (I) Initiate the “Enhanced Due Diligence,” for example:
  - 1. Obtain the relevant data for the application of registration and trade purpose: Such as, the intended use of the electronic stored value card account, the expected customer transaction and activity information, etc.
  - 2. Obtain further business information from customers: Learn about customer business contacts.
  - 3. Obtain instructions and information on the transaction to be completed or already completed.
  - 4. Conduct a field visit or telephone interview based on the classification of customers to confirm the actual operation of customers.
- (II) Before establishing or adding a business relationship, the electronic stored value card issuers shall obtain the approval of the senior management that is authorized according to the internal risk considerations.
- (III) Increase the frequency of customer due diligence.
- (IV) The business relationship shall be supervised forcefully and continuously. Except for the proviso stated in Section, 3, Paragraph 1, Article 6, for a transaction with lower risk, the electronic stored value card issuers may base on the risk prevention policies and procedures to adopt the simplified measures. This simplified measure should be commensurate with the lower risk, and the simplified measure should be adopted as follows:
  - (I) Reduce the frequency of customer 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 of the business relationship 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.

VIII. Electronic stored value card issuers should establish regular and comprehensive risk assessment activities for money laundering and terrorism financing, and prepare risk assessment reports so that the management can understand the overall risk of money laundering and terrorism financing faced by the electronic stored value card issuers in a timely and effective manner in order to determine the mechanism to be established and to develop appropriate counter measures. Electronic stored value card issuers should establish regular and comprehensive money laundering and terrorism financing risk assessment operation based on the following indicators:

- (I) The nature, scale, diversity, and complexity of the business operation
- (II) Targeted market
- (III) Electronic stored value card issuers trading volume and scale: Consider the general trading activities of the electronic stored value card issuers and the characteristics of the customers.
- (IV) High-risk related management data and reports: Such as, the number and proportion of high-risk customers; the amount, quantity, or proportion of high-risk products, services, or transactions; the nationality, place of registration, or place of business of the customer, or the amount or ratio of the transaction in an area involving high-risk, etc.
- (V) Business and products, include the channel and manner of providing business and products to customers, the implementation of customer due diligence, such as, the use of information systems and whether the due diligence is commissioned to a third party or not.
- (VI) Internal audit and the inspection results of the competent authorities

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

- (I) Management reports provided by internal management of the electronic stored value card issuers (such as, business unit managers, customer relationship managers, etc.)
- (II) Anti-Money Laundering and Countering Terrorism Financing Report issued by International Anti-Money Laundering Organizations and other countries.
- (III) The information on the money laundering and terrorism financing issued by the competent authorities

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

Electronic stored value card issuers while experiencing major changes, such as, major events, significant developments in management and operations, or emerging of new threats related to major changes should have the assessment operation initiated again.

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 by the electronic stored value card issuers.

- IX. The policies of the electronic stored value card issuers 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 Stored Value Card Issuers” should be implemented with the approval of the Board of Directors (Executives). Also, it should be submitted to the Financial Supervisory Commission for future reference along with the Guidelines for Anti-Money Laundering and Countering Terrorism Financing. Also, it should be reviewed annually, same for the amendments.