Content

| | |
|---|---|
| Title： | Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for the Third-Party Payment Enterprises Ch |
| Date： | 2022.01.28 |
| Legislative： | 1.Promulgated on January 28, 2022 |
| Content： | Article 1<br>These Regulations are enacted pursuant to paragraph 3 of Article 6, the preceding section of paragraph 4 of Article 7, paragraph 3 of Article 8, paragraph 3 of Article 10 of the Money Laundering Control Act (hereinafter referred to as the “Act”) and paragraph 5 of Article 7 of the Counter-Terrorism Financing Act.<br>Article 2<br>Terms used in these Regulations are defined as follows:<br>1. “Third-party payment enterprise” shall mean a business that is not an electronic payment institution, as defined in the Act Governing Electronic Payment Institutions, and which provides the service of collecting and making payments for online real transactions as an agent.<br>2. “Buyer-side customer” shall mean the payer in an online real transaction.<br>3. “Seller-side customer” shall mean the payee in an online real transaction.<br>4. “Customers” shall mean the buyer-side customer and the seller-side customer in an online real transaction, in which payment collecting and making is done on an agent basis.<br>5."High risk country or region" shall mean a country or region as described in Article 11, paragraph 2 of the Act.<br>A third-party payment enterprise shall not sign contracts with other third-party payment enterprises to be payers or payees.<br>Article 3<br>A third-party payment enterprise shall take appropriate steps every two years to identify, assess, and understand their money laundering/terrorist financing (ML/TF) risks, including at least the seller-side customer, countries or geographic areas, services and transactions or payment channels, and in accordance with the following provisions:<br>1.Make the risk assessment reports available and update them.<br>2.Consider all the relevant risk factors before determining what the level of overall risk is and the appropriate mitigation measures to be applied, including the results of national risk assessment.<br>3.Provide risk assessment reports when requested by the Ministry of Economic Affairs (MOEA).<br>Article 4<br>A third-party payment enterprise shall comply with the following provisions:<br>1.Have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified by the country or by themselves.<br>2.Monitor the implementation of those controls and enhance them if necessary.<br>3.Take enhanced measures to manage and mitigate the risks where higher risks are identified.<br>Article 5<br>A third-party payment enterprise shall establish internal control and audit systems based on their ML/TF risks and business scale, and the systems shall include the following:<br>1.Operations and control procedures of anti-money laundering and countering the financing of terrorism (AML/CFT).<br>2.Holding or participating in on-the-job training related to AML/CFT |

regularly.
3.The responsible person or a designated dedicated person shall be responsible for coordinating and monitoring the implementation of subparagraph 1.
4.Making AML/CFT risk assessment reports available and updating them regularly.
5.Audit procedures.
The on-the-job training referred to in subparagraph 2 of the preceding paragraph shall be proceeded with one of the following methods:
1.The responsible person or a designated dedicated person shall participate in on-the-job training related to AML/CFT held by government, legal persons, or groups at least once every two years.
2.The enterprise shall hold on-the-job training related to AML/CFT at least once every two years. The training may be arranged in combination with other professional training programs.
The audit procedures referred to in subparagraph 5 of paragraph 1 shall, based on the ML/TF risks and business scale, be conducted by means of self-review or internal audit.
The MOEA shall annually conduct sample audits of the implementation of the systems referred to paragraph 1. The audit methods include on-site and off-site inspection. The MOEA may delegate the inspections to another agency, institution, legal person or organization with inspection capability to carry out the inspections.
Article 6
A third-party payment enterprise shall assess the ML/TF risks prior to development of new services and new business practices, including new payment mechanisms, and the use of new or developing technologies for both new and pre-existing services, and take appropriate measures to manage and mitigate those risks.
Article 7
A third-party payment enterprise shall comply with the following provisions in undertaking customer due diligence (CDD) measures:
1.A third-party payment enterprise shall undertake CDD measures when:
(1)establishing or maintaining business relations with seller-side customers;
(2)providing services for buyer-side customer when any transaction reaches NT$50,000. However, this shall not apply to transactions paid by credit card in an amount of less than NT$200,000.
(3)there is a suspicion of money laundering or terrorist financing; or
(4)the third-party payment enterprise has doubts about the veracity or adequacy of previously obtained customer identification data.
2.The CDD measures to be taken by a third-party payment enterprise are as follows:
(1)Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. In addition, a third-party payment enterprise shall retain copies of the customer's identity documents or record the relevant information thereon.
(2)The CDD measures shall include understanding and, as appropriate, obtaining information on, the purpose and intended nature of the business relationship.
3.When the customer is a legal person, an organization or a trust, a third-party payment enterprise shall understand the business nature of the customer and obtain relevant information to verify the customer identity.
4.Where a third-party payment enterprise is unable to complete the required CDD process on a customer, the third-party payment enterprise shall consider filing a suspicious transaction report (STR) on money laundering or terrorist financing in relation to the customer.
5.If a third-party payment enterprise forms a suspicion of money laundering or terrorist financing and reasonably believes that performing the CDD process will tip-off the customer, it is permitted not to pursue that process and file a STR instead.
Article 8
If there exists any of the following situations in the CDD process, a third-party payment enterprise shall consider declining to establish a business relationship or provide any service with the customer:
1.The customer is suspected of opening an anonymous account or using a fake

name, a nominee, a shell firm, or a shell corporation or entity to use the service;
2.The customer refuses to provide documents related to CDD measures;
3.The customer uses forged or altered identification documents;
4.The customer provides only photocopies of the identification documents. However, this does not apply to business for which a photocopy or image file of the identification document supplemented with other control measures are acceptable under applicable rules;
5.Documents provided by the customer are suspicious or unclear, or the customer refuses to provide other supporting documents, or the documents provided cannot be authenticated;
6.The customer procrastinates in providing identification documents in an unusual manner;
7.The customer is an individual, a legal person or an organization sanctioned under the Counter-Terrorism Financing Act, or a terrorist or terrorist group identified or investigated by a foreign government or an international organization, except for payments made under subparagraphs 2 to 3 of paragraph 1 of Article 6 of the Counter-Terrorism Financing Act; or
8.Other unusual circumstances exist in the process of establishing a business relationship or providing services and the customer fails to provide reasonable explanations.

Article 9

A third-party payment enterprise shall conduct ongoing due diligence on the business relationship with seller-side customer and observe the following provisions:
1.A third-party payment enterprise shall scrutinize services undertaken throughout the business relationship to ensure that the services being provided are consistent with the third-party payment enterprise's knowledge of the seller-side customer, its business and risk profile.
2.A third-party payment enterprise shall periodically review the existing records to ensure that documents, data or information of the seller-side customer collected under the CDD process are kept up-to-date, particularly for higher risk categories of seller-side customers, whose reviews shall be conducted at least once every two years.
3.A third-party payment enterprise shall apply CDD requirements to existing seller-side customers on the basis of materiality and risk, and after taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained, conduct due diligence on such existing relationships at appropriate times, including when learning of any material change to the seller-side customer's identity and background information.
4.A third-party payment enterprise may rely on existing customer records to undertake identification and verification. Therefore, a third-party payment enterprise is allowed to provide services without repeatedly identifying and verifying the identity of an existing seller-side customer. However, a third-party payment enterprise shall conduct CDD measures again in accordance with Article 7 herein if he or she has doubts about the veracity or adequacy of the records, such as, where there is a suspicion of ML/TF in relation to that seller-side customer, or where there is a material change in the way that the seller-side customer's transactions or account are operated, which is not consistent with the seller-side customer's business profile.

Article 10

A third-party payment enterprise shall determine the extent of applying CDD and ongoing due diligence measures under subparagraph 2 of Article 7 and the preceding article using a risk-based approach (RBA):
1.For higher risk circumstances, a third-party payment enterprise shall perform enhanced CDD or ongoing due diligence measures by adopting additionally at least the following enhanced measures:
(1)Obtaining the approval of senior management before establishing or entering a new business relationship;
(2)Taking reasonable measures to understand the sources of wealth and the source of funds of the customer; in case the source of funds is deposits, understanding further the source of deposits; and
(3)Conducting enhanced ongoing monitoring of business relationship.
2.For customers from high risk countries or regions or customers on the

sanction list published by the Ministry of Justice pursuant to the Counter-Terrorism Financing Act, a third-party payment enterprise shall conduct enhanced CDD measures consistent with the risks identified.
3.For lower risk circumstances, a third-party payment enterprise may apply simplified CDD measures, which shall be commensurate with the lower risk factors. However simplified CDD measures are not allowed in any of the following circumstances:
(1)Where the customers are from high risk countries or regions; or
(2)Where there is a suspicion of money laundering or terrorist financing in relation to the customer or the transaction.
Article 11
When conducting CDD measures, a third-party payment enterprise shall query the customer and use an external database or information obtained from external sources to determine whether a customer and its senior managerial officer is a person who is or has been entrusted with a prominent function by a domestic government, a foreign government or an international organization (referred to as politically exposed persons (PEPs) hereunder) and shall comply with the following provisions:
1.For a customer determined to be a current PEP of a domestic or foreign government or international organization, a third-party payment enterprise shall treat the customer directly as a high-risk customer, and adopt enhanced CDD measures as specified in the subparagraphs of Article 9.
2.For a senior managerial officer of a customer determined to be a current PEP of the domestic government, a foreign government or an international organization, a third-party payment enterprise shall determine whether to apply the enhanced CDD measures under subparagraphs of Article 9 considering the officer’s influence on the customer.
3.The preceding subparagraphs also apply to family members and close associates of PEPs. The scope of family members and close associates mentioned above will be determined in the manner stipulated in the latter section of paragraph 4 of Article 7 of the Act.
Article 12
A third-party payment enterprise shall report to the Investigation Bureau of the Ministry of Justice (MJIB) pursuant to paragraph 1 of Article 10 of the Act when a transaction includes any of the following circumstances, which raise suspicion of ML/TF and the same shall apply to attempted transactions:
1.When the third-party payment enterprise provides the service of collecting and making payments for online real transactions as an agent for the seller-side customer, and the seller-side customer cannot provide a concrete explanation, or the explanation provided is obviously not true.
2.After the entrusted relationship with the seller-side customer is ended, the third-party payment enterprise discovers that the customer denies the transaction, or that no such customer exists, or that there are sufficient evidences or facts to prove that the customer's name was falsely used by someone else.
3.The buyer-side customer, without due reason, conducts non-credit card transactions with an amount slightly lower than NT$50,000, or pays an amount slightly lower than NT$200,000 by credit card, multiple times or consecutively.
4.The customer conducts an unusual transaction and such transactions do not appear to be commensurate with the customer’s status and income or is unrelated to the nature of the customer’s business.
5.The customer is a natural person, legal person or group that has been announced and sanctioned by the Ministry of Justice pursuant to the Counter-Terrorism Financing Act, or a country announced by the Ministry of Justice, or a terrorist organization or a terrorist recognized or investigated by an international organization.
6.The transaction is suspected to be involved with any terrorist activity, terrorist organization, terrorism financing or financing of proliferation.
7.Other transactions which raise suspicion of money laundering or terrorist financing.
Article 13
A third-party payment enterprise shall keep records on all business relations and services with the customers and in accordance with the following provisions:

1.A third-party payment enterprise shall maintain all necessary records on services for at least five years or for a longer period as otherwise required by law.
2.A third-party payment enterprise shall keep all the following information for at least five years, or for a longer period as otherwise required by law, after the business relationship is ended:
(1)All records obtained through CDD measures, such as copies or records of official identification documents such as passports, identity cards, driving licenses, national health insurance card or similar documents.
(2)Bank account files, proof of payment, or contract files.
(3)Business correspondence, including inquiries to establish the background and purpose of complex, unusual transactions, and the information obtained and the results of any analysis undertaken.
3.Transaction records maintained by a third-party payment enterprise must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.
4.A third-party payment enterprise shall ensure that transaction records and CDD information will be available swiftly to the competent authorities when such requests are made with appropriate authority.
Article 14
A third-party payment enterprise shall file suspicious transaction reports in accordance with following provisions for transactions suspected of involving ML/TF:
1.Within 2 business days upon recognition of a suspicious transaction, a third-party payment enterprise shall file a report to the MJIB.
2.For obviously significant suspicious transactions of an urgent nature, a third-party payment enterprise shall file a report immediately to the MJIB by fax or other available means and follow it up with a written report. However, the third-party payment enterprise is not required to submit a follow-up written report if the MJIB has acknowledged receipt of the report by sending a reply by fax. In such event, the third-party payment enterprise shall retain the faxed reply.
3.The formats of the suspicious transaction report and faxed reply mentioned in the preceding two subparagraphs shall be prescribed by the MJIB.
The data reported to the MJIB and relevant transaction records shall be kept in accordance with the preceding article.
Article 15
A third-party payment enterprise shall pay attention to the sanctions list announced by the Ministry of Justice referred to in Article 4 and 5 of the Counter-Terrorism Financing Act, and comply with paragraph 1 of Article 7 of the same law, including for attempted transactions.
When a third-party payment enterprise, in the course of business relations, discovers that he or she holds or manages any property or property interests of a designated individual, legal person or entity, or discovers the place where any property or property interests of a designated individual, legal person or entity are located, the third-party payment enterprise shall immediately report to the MJIB.
The reporting records of the preceding paragraph and relevant service records shall be kept in accordance with Article 13.
Article 16
These Regulations shall take effect on January 1, 2023, with the exception of paragraph 4 of Article 13, which shall come into effect on the date of promulgation.

Data Source：Ministry of Digital Affairs Laws and Regulations Retrieving System