Content

Title：	Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for for Enterprises or Persons Providing Third-Party Payment Services Ch
Date：	2024.11.29
Legislative：	1.Promulgated on January 28, 2022 2.Formulated and announced 16 regulations by the Ministry of Digital Affairs, on February 24, 2023. 3.On January 22, 2024, the Ministry of Digital Affairs issued Order No. 1134000041, amending and announcing the text of Articles 5 and 16; adding Article 5-1; except for Article 3, which was amended and announced on February 24, 2023, and took effect from January 1, 2023, the rest of the amendments shall take effect from the date of announcement. 4.Amended on November 29, 2024, the Ministry of Digital Affairs issued Order No. 1134000941.
Content：	Article 1 These Regulations are formulated pursuant to Paragraph 3 of Article 7, the first part of Paragraph 4 of Article 8, Paragraph 3 of Article 10, Paragraph 3 of Article 13 of the Money Laundering Control Act (hereinafter referred to as “the Act”), and Paragraph 5 of Article 7 of the Counter-Terrorism Financing Act. Article 2 The terms used in these Regulations are defined as follows: Enterprises or Persons Providing Third-Party Payment Services (hereinafter referred to as “third-party payment service providers”) refers to a business that is not an electronic payment institutions, as defined in the Act Governing Electronic Payment Institutions, and which provides the service of collecting and making payment for online real transactions as an agent. Customer refers to the buyers and sellers in an online real transaction, in which collecting and making payment is done on an agent basis. High-Risk Countries or Regions refers to countries or regions defined in Paragraph 2 of Article 9 of the Act. Risk-Based Approach refers to the methodology whereby third-party payment service providers shall identify, assess, and understand the money laundering (ML) and terrorism financing (TF) (hereinafter referred to as “ML/TF”) risks to which they are exposed, and take appropriate measures to effectively mitigate such risks. Under this approach, third-party payment service providers should implement enhanced measures for higher-risks situations and simplified measures for lower-risks situations, allocating resources efficiently to reduce identified ML/TF risks in the most appropriate and effective manner. Third-party payment service providers shall not enter into agreements to accept other third-party payment service providers as customers. Article 3 Third-party payment service providers shall take appropriate measures at least once every two years to identify, assess, and understand their ML/TF risks. These measures shall cover aspects such as seller customers, countries or regions, services, and transaction or payment channels and shall be carried out in accordance with the following provisions: Prepare and update risk assessment reports. Consider all relevant risk factors, including the results of national risk assessments, prior to determining the overall risk level and the appropriate measures to mitigate such risks.

Provide risk assessment reports upon request by the Ministry of Digital Affairs (hereinafter referred to as “the Ministry”).

Article 4

Third-party payment service providers shall comply with the following provisions:

Establish policies, controls, and procedures approved by senior management, to manage and mitigate identified ML/TF risks, including those identified by the nation or by the provider itself.

Monitor the implementation of control procedures and strengthen them when necessary.

Implement enhanced measures to manage and mitigate identified higher risks.

Article 5

Third-party payment service providers shall establish internal control and audit systems for anti-money laundering (AML) and countering the financing of terrorism (CFT) in accordance with the scale of their business operations and the level of ML/TF risks. These systems shall include the following:

Procedures and controls for AML/CFT.

Regular hosting of or participation in AML/CFT on-the-job training programs.

Appointment of responsible person or designated personnel to coordinate and supervise the implementation of the measures specified in Subparagraph 1.

Preparation and periodic updates of ML/TF risk assessment reports.

Audit procedures.

The on-the-job training referred to in Subparagraph 2 of the preceding paragraph shall be conducted by third-party payment service providers in one of the following manners:

At least once every two years, the responsible person or designated personnel shall participate in AML/CFT on-the-job training conducted by government agencies, legal entities, or organizations.

At least once every two years, providers shall organize their own AML/CFT training sessions, which may be conducted in conjunction with other professional training programs.

The audit procedures specified in Subparagraph 5 of Paragraph 1 shall be align ed with the level of ML/TF risks, as well as the scale of business operations, and may be conducted through self-assessments or internal audits.

The Ministry may adopt a risk-based approach to conduct audits of third-party payment service providers’ implementation of AML/CFT measures at any time. These audits may be carried out by Ministry personnel or entrusted to appropriate institutions, and may include on-site and off-site inspections. When necessary, the Ministry may designate or require third-party payment service providers to commission professional or technical personnel to audit their AML/CFT implementation and submit a report to the Ministry.

In conducting the audits referred to in the preceding paragraph, the Ministry may direct third-party payment service providers to submit relevant AML/CFT books, documents, electronic records, or other data. Regardless of whether such materials are stored in written, electronic, email, or any other form, they shall be provided, and the providers shall not evade, refuse, or obstruct the audit under any pretext.

Article 6

Prior to launching new services or engaging in new types of business, including new payment mechanisms or the application of new technologies to existing or new business, third-party payment service providers shall conduct ML/TF risk assessments and establish corresponding risk management measures to mitigate the identified risks.

Article 7

Third-party payment service providers shall comply with the following provisions when carrying out customer due diligence (hereinafter referred to as “CDD”) measures:

CDD is required when:

(1)Establishing or maintaining a business relationship with a seller customer.
(2)Providing collecting and making payment services to a buyer customer for transactions of NT$50,000 or more per transaction. This requirement does not apply to credit card payments less than NT$200,000 per transaction.
(3)A transaction suspected of ML/TF occurs during collecting and making payment services.
(4)There are doubts about the authenticity or adequacy of previously obtained customer identification information.
CDD measures shall include the following:
(1)Identify and verify the customer's identity using reliable, independent documents, data, or information, and retain copies or records of the identification documents.
(2)Understand the purpose and intended nature of the business relationship and obtain relevant information as appropriate.
In the case of legal persons, entities, or trusts, third-party payment service providers shall understand the nature of their business and identify the beneficial owner(s). Relevant information must be obtained in accordance with the Ministry's regulations to verify the identities of the customer and their beneficial owner(s).
If unable to complete the CDD process, consider filing a suspicious ML/TF transaction report (a Suspicious Transaction Report, hereinafter referred to as "STR") related to the customer.

If a customer or transaction is suspected of involvement in ML/TF, and there is a reasonable belief that undertaking the CDD process would tip-off the customer, providers may forego such process and file a STR instead.

Article 8
In carrying out CDD, third-party payment service providers shall refuse to establish a business relationship or provide services under any of the following circumstances:
The customer is suspected of using anonymous or pseudonymous identities, dummy accounts, fictitious business or legal persons to conduct transactions or use services.
The customer refuses to provide relevant documents for CDD measures.
The customer possesses forged or altered identity documents.
The customer presents only photocopies of identification documents unless regulations permit the use of photocopies or digital copies of identification documents, provided they are supplemented with other control measures for conducting the business.
The customer provides suspicious, unclear, or unverifiable documents and refuses to submit additional supporting materials.
The customer unreasonably delays the submission of required identity documents.
The customer is listed as a sanctioned individual, legal person, or entity under the Counter-Terrorism Financing Act, or identified or investigated as a terrorist or terrorist group by a foreign government or international organization. However, payments made pursuant to Subparagraphs 2 and 3 of Paragraph 1, Article 6 of the Counter-Terrorism Financing Act are excluded from this provision.

The customer cannot provide reasonable explanations for unusual circumstances during the establishment of a business relationship or provision of services.

Article 9
Third-party payment service providers shall conduct ongoing reviews of seller customer business relationships and comply with the following provisions:
Conduct detailed reviews of services provided within the seller customer's business relationship to ensure alignment with the seller customer's business operations and risk profile.
Periodically review the adequacy of information obtained for identifying seller customers, ensuring the information is updated. For high-risk seller customers, such reviews shall be conducted at least

once every two years.
Review the identity information of existing seller customers based on significance and risk level. After considering the timing of the previous review and the adequacy of the information obtained, a review of existing relationships should be conducted at appropriate times, including when significant changes are known regarding the seller customer's identity or background information.
For identification and verification procedures for seller customers, previously executed and stored data may be relied upon without re-verifying the seller customer’s identity for each service use. However, when there are doubts about the authenticity or adequacy of the seller customer’s information, indications of ML/TF transactions, or material changes in transactions or account operations that are inconsistent with the seller customer’s business nature, identity verification must be conducted again as per Article 7.

Require seller customers to retain relevant evidence of online real transactions and have periodical verification in process.

Article 10
When carrying out CDD measures and ongoing review mechanisms pursuant to Subparagraph 2 of Article 7, and the preceding article, third-party payment service providers shall determine the level of implementation based on a risk-based approach, including:
For high-risk scenarios, enhanced CDD or ongoing review measures shall be implemented, including at least the following:
(1) Obtaining approval from senior management prior to establishing or expending business relationships.
(2) Taking reasonable measures to understand the customer’s source of wealth and source of funds. “Source of funds” refers to the actual origin of the funds.
(3) Applying enhanced ongoing monitoring to the business relationship.
For customers from high-risk countries or regions, apply enhanced measures proportionate to the identified risk.
For lower-risk scenarios, simplified customer identification measures may be applied, provided that such measures are commensurate with the identified lower-risk factors. However, simplified customer identification measures shall not be applied under the following circumstances:
(1) The customer is from a high-risk country or region.
(2) There are reasonable grounds to suspect that the customer or transaction involves ML/TF.

Article 11
In carrying out CDD measures, third-party payment service providers shall inquire with the customer and utilize external databases or information sources to verify whether the customer or its senior management is a current or former politically exposed person (hereinafter referred to as “PEP”) entrusted with a prominent public function in a domestic or foreign government or international organization . The following provisions shall apply:
If a customer is a current PEP holding a prominent public function in a domestic or foreign government, they shall be directly classified as a high-risk customer, and the enhanced CDD measures set forth in Article 9 shall be applied.
If a senior management member of the customer is currently a PEP in a domestic or foreign government or international organization, their influence on the customer shall be assessed to determine whether to apply the enhanced CDD measures outlined in Article 9.

The provisions of the preceding two subparagraphs shall also apply to family members and close associates of PEPs. The scope of family members and close associates shall be determined in accordance with the standards set forth in the latter part of Paragraph 4 of Article 8 of the Act.

Article 12
Third-party payment service providers shall file a report with the Investigation Bureau of the Ministry of Justice (hereinafter referred to as

the "Investigation Bureau") pursuant to paragraph 1 of Article 13 of the Act for any service or transaction suspected of ML/TF, even if the transaction is not completed. This includes:

Providing collection and making payment services for online real transactions where the seller customer fails to provide proof of the online real transactions, or the proof is evidently false.

Discovering, after the termination of a relationship with a seller customer, that the customer denies the delegation, is non-existent, or there is factual evidence indicating that the customer's identity has been impersonated.

Buyer customers conducting multiple or consecutive transactions just below NT$50,000 for non-credit card payments or just below NT$200,000 for credit card payments without justification.

Transactions that are unusual and clearly disproportionate to the customer's identity, income, or the nature of their business.

Customers identified as individuals, legal persons, or entities sanctioned by the Ministry of Justice under the Counter-Terrorism Financing Act, or identified or investigated as a terrorist organization or terrorist by other countries or international organizations announced by the Ministry of Justice.

Transactions suspected of being linked to terrorist activities, terrorist organizations, financing of terrorism, or weapons proliferation.

Any other suspected ML/TF transactions.

Article 13

Third-party payment service providers shall retain records of customer interactions and services provided in accordance with the following provisions:

All necessary records related to services shall be retained for at least five years unless otherwise specified by laws requiring a longer retention period.

The following data shall be retained for at least five years after the termination of the customer relationship, unless otherwise specified by laws requiring a longer retention period:

(1) All records obtained through CDD measures, such as copies or records of passports, national identification card, driver's licenses, national health insurance card, or similar official identification documents.

(2) Bank account information, payment proofs, or contract documents.

(3) Business correspondence, including background or purpose information obtained from inquiries into complex or unusual transactions, and the results of any analysis undertaken.

The retained transaction records shall be sufficient to reconstruct individual transactions, serving as evidence for identifying illicit activities when necessary.

Upon request by the competent authority, third-party payment service providers shall ensure the prompt provision of collecting and making payment records and CDD information.

Article 14

Third-party payment service providers shall report suspected ML/TF transactions in accordance with the following provisions:

When a transaction is identified as suspected of ML/TF, a STR shall be filed with the Investigation Bureau within two business days.

For obviously significant and urgent suspected ML/TF transactions, a report shall be filed immediately by fax or other feasible means, followed by submission of a written report. If the Investigation Bureau confirms receipt of the report via fax acknowledgment, no follow-up written report is required, but the fax acknowledgment shall be retained.

The formats of STR and fax acknowledgment shall be in accordance with the format prescribed by the Investigation Bureau.

The retention period for records of reports submitted to the Investigation Bureau shall comply with the provisions of Subparagraph 1 of the previous

	Article. Article 15 Third-party payment service providers shall monitor the sanctions lists announced by the Ministry of Justice pursuant to Articles 4 and 5 of the Counter-Terrorism Financing Act and act in accordance with Paragraph 1 of Article 7 of the same Act. The same applies to incomplete services. If a third-party payment service provider becomes aware, through the course of its business, that it holds or manages the properties or property interests of a designated sanctioned individual, legal person, or entity, or the location of such properties or property interests, it shall promptly submit such information to the Investigation Bureau in the format and manner specified by the bureau. The retention period for such reporting records shall comply with the provisions of Subparagraph 1 of Article 13. Article 16 These Regulations shall enter into force on November 30, 2024.

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