


Content

Title :	Regulations Governing the Identification and Control Measures for Customers Suspected of Fraud for Third-Party Payment Service Providers 
Date :	2024.11.29
Legislative :	Announced on November 29, 2024.
Content :	<p>Article 1</p> <p>These Regulations are formulated in accordance with Paragraph 3 of Article 34 and Paragraph 3 of Article 35 of the Fraud Crime Hazard Prevention Act (hereinafter referred to as “the Act”).</p> <p>Article 2</p> <p>The criteria for identifying customers suspected of involving in fraud crimes (hereinafter referred to as “suspected fraudulent customers”) according to Paragraph 1 of Article 34 of the Act are as follows:</p> <p> Holders of third-party payment accounts that have been reported by courts, prosecutor’ s offices, or the judiciary police department as accounts suspected of fraud crimes (hereinafter referred to as “flagged fraudulent accounts”).</p> <p> Holders of third-party payment accounts that have been referred by financial institutions or other third-party payment service providers as accounts suspected of fraud crimes (hereinafter referred to as “suspected fraudulent accounts”).</p> <p> Customers otherwise involving in fraud crimes identified by third-party payment service providers by comprehensive assessment of factors, such as the customer’ s business model, business scale, transaction methods, industry risk of being exploited for fraud, and public reports of suspicious transactions.</p> <p>Article 3</p> <p>Third-party payment service providers shall establish internal fraud prevention measures, which shall include the following:</p> <p> Defining patterns for identifying suspected fraudulent customers based on the factors specified in Subparagraph 3 of the preceding article and the fraudulent patterns published by competent authorities or industry associations.</p> <p> Adopting appropriate measures to identify, assess, and understand fraud risks, including at least customers, services, transactions, and payment channels, and formulating early warning norms and verification procedures for internal fraud prevention measures.</p> <p> Adopting necessary enhanced management measures for high-risk customers and transactions.Third-party payment service providers shall regularly review the implementation of internal fraud prevention measures and finalize the prepare assessment reports; if deficiencies are found, improvements shall be made.</p> <p>Third-party payment service providers shall regularly review the implementation of internal fraud prevention measures and finalize the prepare assessment reports; if deficiencies are found, improvements shall be made.</p> <p>Article 4</p> <p>For suspected fraudulent customers, third-party payment service providers shall enhance identity verification processes by implementing all or part of the following ac-tions:</p> <p> Requesting customers to provide ad-ditional supporting documents suffi-cient to verify their identity and the source of funds.</p> <p> Conduct on-site inspection, video calls, or voice calls to verify the customer’ s status.</p> <p> Cross-referencing with information provided by financial institutions or other trusted sources to verify the customer’ s identity.</p> <p>In addition to complying with the pro-visions of the preceding paragraph,</p>

third-party payment service providers may adopt the following measures for ongoing identity review of customers:

- Verifying that the customer's transactions align with their business activities, and when necessary, ascertaining the source of funds or confirming the legitimacy of the transactions.

- Reviewing the adequacy of the information obtained for identifying the customer's identity, ensuring its timeliness, accuracy, and appropriateness.

- Continuously monitoring the customer's transactions or account operations for any potential involvement in fraud crimes.

Article 5

If any of the following circumstances occur to a suspected fraudulent customer, third-party payment service providers may refuse to establish a business relationship or provide services:

- Refusing to cooperate with the procedures set forth in the preceding article or to provide relevant documents required for identity verification processes.

- Suspected use of anonymous or pseudonymous identities, nominee accounts, fictitious business or legal entities to conduct transactions or use services.

- Possessing forged or altered identity documents.

- Providing suspicious, vague, or unverifiable documents and refusing to submit additional supporting materials.

- Unreasonably delaying the submission of required identity documents, registration certificates, or other approval documents.

Article 6

If a suspected fraudulent customer refuses to cooperate with the procedures set forth in Article 4, or is verified to be involved in fraud crimes, third-party payment service providers may suspend the appropriation of transaction funds within the customer's account or suspend the provision of services.

The period of suspension of appropriation or services of the preceding paragraph shall not be less than 20 days.

Article 7

Third-party payment service providers, according to Paragraph 1 of Article 35 of the Act, shall promptly report information related to suspected fraudulent customers to the judiciary police department in the customer's locality through one of the following methods:

- Mailing or sending it to the address or email designated by the judiciary police department.

- Reporting it via the website designated by the judiciary police department.

Article 8

If a third-party payment service provider identifies a customer suspected of involving in fraud crimes, it may notify industry peers in writing or electronically.

The notification of the preceding paragraph shall include details such as the customer's name, address, identity document number, and other relevant identifying information of the suspected fraudulent customer. If the customer is a company or business entity, the notification shall include its name, registered address, registration number, as well as the name, address, and identity document number of its representative.

Article 9

When a third-party payment service provider suspend the suspected fraudulent customers' appropriation of funds according to Article 6 and reports the case to the judiciary police department, the department shall, within 20 days of receiving the report, notify the provider to carry out the subsequent control or cancel the control over the postponed appropriation.

For major and urgent cases, the judiciary police department may issue the notification mentioned in the preceding paragraph via phone, fax, email, or other feasible means, and shall deliver the formal written documents to the third-party payment service provider within five business days after the notification.

When a third-party payment service provider implements subsequent control measures according to the first paragraph, it shall, based on the control

period specified by the judiciary police department (no more than two years), delay the payout of transaction funds in the suspected fraudulent customer's account and suspend the provision of services.

Article 10

Upon receiving a report of a flagged fraudulent account from the judiciary police department, the third-party payment service provider shall promptly check transactions associated with the account. If the third-party payment service provider finds that the fraudulent funds referenced in the report have been remitted, it shall notify the receiving bank and the original reporting agency, providing details of the remitted funds and the name of the reporting agency.

The procedures of the preceding paragraph shall apply when third-party payment service providers receive notifications of suspected fraudulent accounts from financial institutions.

Article 11

Upon receiving a report according to Paragraph 1 of the preceding article, third-party payment service providers shall suspend the appropriation of transaction funds or suspend to provide services for the flagged fraudulent account. The control period shall commence from the date of the judiciary police department's report and shall automatically expire after two years. However, if continued control is deemed necessary, the original reporting agency shall issue a renewed report prior to the expiration of the control period, and the control period will be extended once up to one year.

Article 12

If a flagged or suspected fraudulent account is released from control by the judiciary police department or upon expiry of the control period, third-party payment service providers shall lift the account's restrictions.

If a customer believes their account is not a flagged fraudulent account or that the circumstances involving fraud no longer exist, they may file a written appeal with supporting evidence to the judiciary police department. The department shall notify the applicant of the appeal's outcome and concurrently inform the third-party payment service provider.

If a customer believes their account is not a suspected fraudulent account or that the circumstances involving fraud no longer exist, they may file a written appeal with supporting evidence to the third-party payment service provider. If the provider investigates and confirms the claim, it shall report to the judiciary police department and recommend lifting the restrictions.

Article 13

Third-party payment service providers shall keep the data obtained from identity verification procedures and transaction records for suspected fraudulent customers as follows:

All necessary transaction records shall be retained for at least five years. However, if other laws stipulate longer retention periods, those regulations shall prevail. These records include:

- (1) Information related to actual transactions, such as transaction dates, types, amounts, and categories.
- (2) Identity information of the payer and recipient.
- (3) Methods of fund deposit and payout used in payment services.
- (4) Methods of identity verification.
- (5) Records of notifications and reports regarding suspected fraudulent customers and their suspicious transactions.

The following data shall be retained for at least five years after the termination of the customer relationships. However, if other laws stipulate longer retention periods, those regulations shall prevail:

- (1) All records obtained through identity verification processes.
- (2) Account and account number 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 fraud crimes when necessary.

Upon request by the competent authority, third-party payment service providers shall ensure the prompt provision of payment collection and payout records and information of identity verification processes.

Article 14

These Regulations shall enter into force on November 30, 2024.

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