Regulations Governing Identity Verification Mechanism and Transaction Limits for Users of Electronic Payment Institutions

Chapter 1 General Provisions

Article 1 These Regulations are adopted pursuant to Paragraph 4 of Article 15, Paragraph 3 of Article 24, Paragraph 3 of Article 25, Article 39 and Article 40 to which Paragraph 4 of Article 40 applies *mutatis mutandis*, Paragraph 3 of Article 24, and Paragraph 3 of Article 25 of the Act Governing Electronic Payment Institutions (referred to as the “Act” hereunder).

Article 2 The terms as used in these Regulations are defined as follows:

1. "Users" shall mean persons who register and open an electronic payment account (referred to as "e-payment account" hereunder) with an electronic payment institution and use the services provided by the electronic payment institution to make funds transfer or deposit stored value funds.
2. "E-payment account" shall mean an online account opened by users with an electronic payment institution to keep track of their funds transfer and funds deposit records
3. "Individual user" shall mean natural person users, including foreign natural persons and Mainland Area natural persons.
4. "Non-individual user" shall mean government agencies, legal persons, business entities and other organizations in the ROC as well as foreign legal persons and legal persons in Mainland Area.

Chapter 2 Manner of Establishment, Process for and Management of User Identity Verification Mechanism

Article 3 When an electronic payment institution accepts user registration, it shall know the identity of user, save the identity information of user and confirm the veracity of user identity information according to these Regulations; the preceding provision applies when a user changes his/her identity information.

An electronic payment institution should ask users to provide truthful identity information and shall not accept user registration without a name or using fictitious name.

Article 4 When an electronic payment institution accepts a user application for registration, it shall make an inquiry with the Joint Credit Information Center ("JCIC) for the following information and save relevant records for future reference:

1. Information on deposit account with suspicious or unusual transactions

2. Data and information reported by electronic payment institutions pursuant to Subparagraphs 2 and 3, Paragraph 1, Article 21 of the Rules Governing Business Management of Electronic payment institutions.
3. Notation data where the principal requests enhanced identity verification.
4. Other data as required by the competent authority.

Electronic payment institutions shall make prudent use of data obtained in the inquiry made according to the preceding paragraph and decide whether to approve or reject user's registration application based on objectivity and autonomy.

Article 5 An electronic payment institution shall reject a user's application for registration if the user has any of the following situations:

1. The applicant uses forged or altered identification document, registration paper or license or relevant approval documents.
2. The applicant is suspected of using a fake name, a dummy , or a bogus business entity or a dummy corporation to apply for registration.
3. Documents provided by the applicant are suspicious or illegible, or the applicant refuses to provide other supporting documents, or the documents provided cannot be authenticated.
4. The applicant procrastinates in providing identification document, registration paper or license or relevant approval documents without justification.
5. The application is made through mandate or power of attorney, but verification of the fact of mandate or power attorney and related identity information is difficult.
6. The same payment instrument provided for identity verification has been used repeatedly by different users for identity verification.
7. The user has the record of unlawfully using a bank deposit account or e-payment account as reported by relevant agencies.
8. Other situations under which user's application shall be rejected as provided by the competent authority.

An electronic payment institution may reject a user's application for registration if the user has any of the following situations:

1. The deposit account has been reported as a watch-listed account and the account status has not been removed.
2. The applicant applies for registration frequently over a short period of time without reasonable explanation.
3. The transaction functions applied for are obviously inconsistent with the applicant's age or background.
4. Data obtained from inquiry with JCIC according to Paragraph 1 of the preceding article show irregularity.

5. The same mobile phone number, email address or social medial account number provided for identity verification has been used repeatedly in identity verification without reasonable explanation.
6. Other situations under which user's application may be rejected as provided by the competent authority.

Article 6 The types and transaction functions of e-payment accounts opened by users with an electronic payment institution are as follows:

1. Type 1 e-payment account: An e-payment account for individual users that offers the functions of collecting and paying funds for real transactions and accepting deposit of stored value funds but without the function of accepting payments or fund transfer between e-payment accounts.
2. Type 2 and 3 e-payment account: An e-payment account for individual users and non-individual users that offers the functions of accepting payments, making payments and accepting deposit of stored value funds.

The e-payment account of individual users who have not completed the identity verification process set out in Subparagraph 3, Paragraph 1 of Article 8 herein may not offer the function of accepting deposit of stored value funds.

Article 7 When accepting individual user registration, an electronic payment institution shall ask the user to provide basic identity information, including at least name, nationality, type and number of identification document and date of birth.

Article 8 When an electronic payment institution accepts individual users to register and open a Type 1 e-payment account, its identity verification process shall comply with the following provisions:

1. Verifying the mobile phone number provided by user;
2. Verifying the email address or social media account provided by user; and
3. When national ID card is provided, checking the user's ID card issuance record with the Ministry of the Interior or JCIC to verify data veracity; when resident certificate is provided, checking the veracity of data with the Ministry of the Interior.

For users whose identity cannot be verified according to Subparagraph 3 of the preceding paragraph, payment should be made in a manner where the movement of funds is traceable.

Payment made in a manner where the movement of funds is traceable mentioned in the preceding paragraph shall be limited to transfer of funds from deposit account, credit card charges or other payment methods approved by the competent authority.

Article 9 When an electronic payment institution accepts individual users to register and open a Type 2 e-payment account, its identity verification process shall comply with the following provisions:

1. Carrying out the procedure specified in Paragraph 1 of the preceding article; and
2. Confirming the payment instruments used by user.

The payment instruments referred to in Subparagraph 2 of the preceding paragraph shall be limited to deposit account, credit card or other payment instruments recognized by the competent authority, excluding deposit accounts not opened over-the-counter or opened after identity verification based on a certificate that complies with the Electronic Signatures Act.

Article 10 When an electronic payment institution accepts individual users to register and open a Type 3 e-payment account, its identity verification process shall comply with the following provisions:

1. Carrying out the procedure specified in the preceding article; and
2. Verifying the user identity via over-the-counter review or based on a certificate that complies with the Electronic Signature Act.

Article 11 When accepting non-individual user registration, an electronic payment institution shall ask the user to provide basic identity information, including at least name of entity, country of registration, registration paper, license or type and number of approval document for establishment, contact information, as well as representative's nationality, type and number of identification document, mailing address and telephone number.

Article 12 When an electronic payment institution accepts non-individual users to register and open a Type 2 e-payment account, its identity verification process shall comply with the following provisions:

1. Verifying the email address provided by user;
2. Confirming the payment instruments used by user; and
3. Requesting the image file on user's registration paper or license or approval document for establishment, and representative's identification document.

Paragraph 2 of Article 9 herein applies *mutatis mutandis* to payment instruments provided in Subparagraph 2 of the preceding paragraph.

With respect to the image file on registration paper or license or approval document for establishment requested from onshore non-individual users in accordance with Subparagraph 3 of Paragraph 1 hereof, the electronic payment

institution shall check the registration data with the Ministry of Economic Affairs, Ministry of Finance or the competent authority in charge of user's line of business.

Article 13 When an electronic payment institution accepts non-individual users to register and open a Type 3 e-payment account, its identity verification process shall comply with the following provisions:

1. Carrying out the procedure specified in the preceding article; and
2. Verifying the user identity via over-the-counter review or a certificate presented by user's representative or its authorized agent that complies with the Electronic Signatures Act.

An electronic payment institution shall verify the actual beneficiary of user in accordance with its directions for anti-money laundering and countering terrorism financing.

Article 14 An electronic payment institution is deemed to have carried out the required identity verification process for an offshore user, provided the offshore outsourced service provider it engages performs user identity verification following a procedure not less than the requirements set out in Articles 8 ~ 10, Article 12 and Article 13 herein.

If an electronic payment institution engages an offshore outsourced service provider to perform the identity verification process, the institution should adopt the following management measures for the offshore outsourced service provider:

1. Taking whether the outsourced service provider is located in high-risk countries or regions known to have inadequate anti-money laundering and countering terrorism financing (AML/CFT) regimes as a consideration to determine whether to engage the outsourced service provider to conduct identity verification process.
2. Making sure that the offshore outsourced service provider is under regulation, supervision or monitoring, and has proper measures in place to ensure compliance with regulations governing customer identity verification and record retention.
3. Making sure that it can access relevant data gathered by the offshore outsourced service provider in identity verification process and establishing relevant mechanism for requiring the offshore outsourced service provider to provide such data without delay.

The term "high risk countries or regions" referred to in Subparagraph 1 of preceding paragraph includes but is not limited to those designated by international organizations on AML/CFT as countries or regions with serious deficiencies in their AML/CFT regime , and other countries or regions that do not or insufficiently

comply with the recommendations of international organizations on AML/CFT as forwarded by the competent authority.

Where an offshore outsourced service provider cannot support the management measures specified in Subparagraphs 2 and 3, Paragraph 2 herein, the electronic payment institution should terminate its service.

Where an electronic payment institution has engaged an offshore outsourced service provider to conduct identity verification process, the electronic payment institution shall still be responsible for the verification of user identity.

Article 15 Electronic payment institutions should, based on the results of differentiated identity verification performed according to these Regulations, set up user risk categorization standards and rate the risk grades of users accordingly, and carry out scheduled or unscheduled monitoring, checking and risk control.

Article 16 Electronic payment institutions should periodically remind users to update their identity information.

Electronic payment institutions should employ certain methods to review user's identity information on a continuous basis and ask users to go through identity verification process again in case of any of the following situations:

1. An individual user or a non-individual user applies to change basic identity information provided in Article 7 or Article 11 herein.
2. The transactions of a user's e-payment account show irregularity.
3. The identification document, registration paper or license or relevant documents provided by the user at the time of registration is suspected of being forged or altered.
4. When a user makes a transaction, it has been one year since the user's last transaction.
5. The same mobile phone number, email address or social media account has been used by different users for identity verification.
6. A transaction is suspected of money laundering or terrorism financing or the money remitted in is from a high risk money laundering or terrorism financing country or region.
7. The institution has doubt about the veracity or appropriateness of the user identity information obtained.
8. Other situations where the institution believes that it is necessary to re-verify the user identity information based on obvious evidence.

When an electronic payment institution reviews the user identity information according to the preceding paragraph, it may use the following means to re-verify the user identity aside from checking the identification document and registration

paper or license or relevant document:

1. Asking the user to provide other identity information.
2. Contact the user by phone, email or in writing.
3. Pay the user a visit.
4. Verify the information with relevant agencies.

For users who fail to cooperate in the re-verification of identity information, an electronic payment institution may suspend their transactions.

Chapter 3 Transaction Limits and Management

Article 17 The transaction limits on e-payment accounts opened by users with an electronic payment institution are as follows:

1. Type 1 e-payment account: Cumulative payment for real transactions shall be limited to an equivalent of NT$30,000 per month; the balance of stored value funds deposited shall be limited to an equivalent of NT$10,000.
2. Type 2 e-payment account: Cumulative payment received and made shall be respectively limited to an equivalent of NT$300,000 per month.
3. Type 3 e-payment account: Cumulative payment received and made for real transactions per month shall be agreed between the electronic payment institution and the user; for individual users, the cumulative payment received and paid via transfer between e-payment accounts shall be respectively limited to an equivalent of NT$1,000,000 per month; for non-individual users, the cumulative payment received and paid via transfer between e-payment accounts shall be respectively limited to an equivalent of NT$10,000,000 per month.

Article 18 When a user opens more than one e-payment account with an electronic payment institution, the amount of payment received and made per account shall not exceed the limit on that type of account, whereas the total limits on those accounts combined shall not exceed the highest limit set for e-payment accounts registered and opened by the same user.

Article 19 Electronic payment institutions that engage in the businesses of accepting deposits of stored value funds and fund transfer between e-payment accounts shall comply with the provisions on limits set out in Paragraphs 1 and 2, Article 15 of the Act and undertake hierarchical user management within the set limits.

Chapter 4 Retention of Data Obtained in User Identity Verification Process and Necessary Transaction Records

Article 20 Electronic payment institutions shall retain the data obtained in user identity

verification process and relevant records on carrying out the user identity verification; the preceding provision applies when users change their identity information.

Article 21 Electronic payment institutions shall retain the following necessary transaction records on users' e-payment accounts:

1. For the business of collecting and making payments for real transactions as an agent: Retain records on the type, account number or card number of payor's payment instrument, amount, currency and time of payment, e-payment accounts of payor and recipient, transaction service fee and transaction results; in case of refunds, retain refund method, amount, currency, time, type, account or card number of payment instrument used for refund payment and transaction results.
2. For the business of accepting deposits of funds as stored value funds: Retain deposit method, e-payment account receiving the deposit, amount, currency and time of deposit, transaction service fee and transaction results; in case of foreign currency deposit, retain the number of foreign-currency deposit account from which the stored value fund is remitted.
3. For the business of transferring funds between e-payment accounts: Retain the numbers of payor and recipient e-payment accounts, amount, currency and time of transfer, transaction service fees and transaction results.
4. For withdrawal of funds from e-payment account: Retain the number of e-payment account from which the fund is withdrawn, the number of same-currency bank deposit account of user into which the fund is transferred, amount, currency and time of withdrawal, transaction service fees and transaction results.

Electronic payment institutions shall retain the log files of necessary transaction records mentioned in the preceding paragraph for at least five (5) years and ensure their veracity and completeness to facilitate account examination and reconciliation.

Chapter 5 Supplemental Provisions

Article 22 For an electronic payment institution that has been engaging in the business of collecting and making payments for real transactions as an agent, if its user identity verification process and transaction limits have not been complying with the provisions in Chapter 2 and Chapter 3 herein with respect to customers to whom it has provided service before and within three months after the Act becomes effective, the institution shall make adjustment to become compliant within 9 months after this Act becomes effective.

During the adjustment period specified in the preceding paragraph, the electronic payment institution shall make sure its users go through at least the following identity verification process before it may start providing the service of collecting and making payments for real transactions as an agent:

1. Verifying the mobile phone number provided by user; and
2. Verifying the email address or social media account provided by user.

For e-payment accounts that have gone through the identity verification process provided in the preceding paragraph only, the cumulative payment for real transactions shall be limited to an equivalent of NT$10,000 per month.

For customers mentioned in Paragraph 1 and users mentioned in Paragraph 2 hereof, an electronic payment institution shall notify them, on a monthly basis and each time service is provided, that they should complete the identity verification process provided in Chapter 2 herein within 9 months after the Act becomes effective, and remind them that should they fail to complete the identity verification process provided in Chapter 2 herein within 9 months after the Act becomes effective, the electronic payment institution will no longer be able to continue to provide services according to their original agreement or the provisions of Chapter 2 herein.

Article 23 These Regulations shall be in force on May 3, 2015.