

Unofficial Translation

with courtesy of the Association of International Banks

This translation is for convenience of those unfamiliar with Thai language.

Please refer to the Thai text for the official version.

Bank of Thailand Notification

No. SorNorChor. 1/2563

Re: Regulations on Know Your Customer (KYC)

For e-Money Service Activation

1. Rationale

Electronic money service (e-Money) is a financial product that offers convenience to the customers for payment of goods or services and funds transfer which obtains continuous popularity. Nowadays, there are various forms of e-Money businesses; and in each form, there are different levels of risks, and the customer's verification process of many business providers fail to perform verification of the identification evidence and the true identity of the customers. Additionally, there are more diversity of the forms of service providing that focus on online channels and application of new technology to making financial transaction to support other types of financial service providing through digital platforms such as borrowing and account opening through digital channel. These may cause the risk of counterfeit or the use of other people's information to activate e-Money service for a purpose of money laundering and fraud.

Business providers must have the process of Know Your Customer (KYC) for e-Money service activation which consists of 2 important steps which are (1) customer identification and (2) customer verification. Besides having duty to comply with the guidelines on KYC under the law governing anti-money laundering, the business providers shall also additionally comply with the process of customer verification according to this Notification. The aforementioned compliance aims at the process of customer verification of business providers to be appropriate and consistent with the risk levels of product and e-Money service activation channels which will help prevent frauds in form of counterfeit or using other people's information, as well as

being the measure for Anti-Money Laundering, Combating Financing of Terrorism and Combating Proliferation Financing (AML/CFT/CPF).

The objectives of the regulations stipulated in this Bank of Thailand Notification are to enhance the ecosystem of KYC to be secure and trustworthy according to the risk levels of product and e-Money service activation channels and to promote the access to other financial services through digital platforms, so that every party is able to provide and use the services altogether with convenience and safety. In this regard, the Bank of Thailand (BOT) has taken into consideration the impartiality in supervision of both financial institution and non-financial institution e-Money business providers.

2. Statutory Power

By virtue of Section 24 of the Payment System Act B.E. 2560 (2017), the Bank of Thailand hereby stipulates the regulations on Know Your Customer (KYC) for e-Money service activation as prescribed in this notification.

3. Scope of Application

This notification shall be applied to the e-Money business providers under supervision in accordance with the law governing the payment system.

4. Content

4.1 Definition

In this notification,

“**Business provider**” means the business provider licensed or registered to undertake the e-Money business under supervision according to the law governing the payment system.

“**Customer**” means a natural person, juristic person or persons with legal agreement to develop the business relationship or make the transaction with the business provider.

“**Person with legal agreement**” means a natural person or juristic person who has legal agreements to possess, utilize, dispose or manage assets by any means for the benefit of another natural person or juristic person.

“**Credible source of information**” means the source of information that provides or develops the information with rationale, criteria or with reference for people or the business groups to examine or have access to various information.

“**BOT**” means The Bank of Thailand under the law governing the Bank of Thailand.

4.2 Regulations on Know Your Customer

4.2.1 To know the customer for e-Money service activation, the business providers must have a process of customer identification to obtain the information and evidence that identify the customer, and customer verification to verify accuracy, genuineness and the valid of identification information and evidence, including the proof that customer is the true owner of such information and evidence. Besides having duty to comply with the regulations on customer identification and customer verification under the law governing anti-money laundering, the business providers shall also additionally comply with the process of customer verification according to this Notification.

4.2.2 For the business providers to establish the process of customer verification for e-Money service activation to be consistent with the risk level of each type of product and e-Money service activation channels, the BOT has stipulated the following regulations:

(1) e-Money service for domestic payment of goods or services.

The business providers who provide domestic e-Money service for payment of goods or services without funds transfer service shall comply with the regulations on customer identification and customer verification in accordance with the law governing anti-money laundering.

(2) e-Money service for payment of goods or services and transfer of funds

The business providers who provide e-Money service for payment of goods or services both domestically and internationally with funds transfer service, or payment of goods or services only internationally, shall additionally comply with the

regulations on customer verification according to this Notification which the business providers shall consider on the basis of the customer activation channel of e-Money service as follows:

(2.1) Face-to -face customer verification

The business providers must examine the accuracy, genuineness and the updates of identification information and evidence of the customer from the reliable source and must prove that the customer is the true owner of such information and evidence. For a case of using the smart ID card as identification evidence, the business providers have to examine the information from the smart card reader and examine the status of the smart ID card through the electronic examination system of the government agencies as well as examining whether the customer is the true owner of such information and evidence.

(2.2) Non face-to -face customer verification

The business providers must examine the accuracy, genuineness and the updates of identification information and evidence of the customer from the reliable source and must prove that the customer is the true owner of such information and evidence. For a case of using the smart ID card as identification evidence, the business providers have to examine the information from the smart card reader and examine the status of the smart ID card through the electronic examination system of the government agencies, as well as taking and recording photos of customers. Furthermore, the high technology of universal standards or standards generally accepted shall be utilized to compare the photo of customer's face with the biometric data obtained from the smart ID card in order to prove that such customer is the true customer as a replacement of having the face-to-face meeting with the customer.

In case where the business providers of e-Money service under Clause 4.2.2 (2) have the measures to manage risk of such e-Money service until it is equivalent to the financial products or services with low risk according to the AMLO's Notification on guidelines for prescribing factors for consideration of low-risk customers, the business providers may examine the accuracy and the validof identification information and evidence from the reliable source of information as well as proving if the customer is the true owner of such information and evidence. For a case of using the smart ID card to be identification evidence, the business providers must examine the status of the smart ID card through the electronic

examination system of the government agencies, as well as examining whether the customer is the true owner of such information and evidence.

In this regard, the business providers shall prescribe other methods in performing customer verification in case where there is a temporary suspension causing the non-compliance with the stipulated regulations for customer verification under Clause 4.2.2 (2), in the risk management measures and internal operation procedures to deal with such situation under Clause 4.3 (5).

4.2.3 Know Your Customer for e-Money service activation in case of juristic persons

Not only the business providers must have a duty to comply with the guidelines on identification and verification of the customers who are juristic persons (corporate customers) according to the law governing anti-money laundering, but they also have to additionally comply with identity verification of person being delegated with final authorization of such corporate customers (if any) under this Notification according to the risk level of each type of product and e-Money service activation channel under Clause 4.2.2.

The business providers may apply other methods of risk management measures on KYC of the corporate customers that are of equivalent assurance level to the guidelines stipulated in this Notification. That is, the business provider may assign the officers who are in charge of or acquainted with such corporate customers to examine the accuracy, genuineness and the valid of identification information and evidence of corporate customers, which can be proved that person activating the service is truly the person delegated with final authorization by such corporate customers (if any).

In this regard, the business providers shall prescribe other methods in performing customer verification in case where there is a temporary suspension causing the non-compliance with the stipulated regulations for customer verification under Clause 4.2.2 (2), in the risk management measures and internal operation procedures to deal with such situation under Clause 4.3 (5).

4.2.4 Customer verification through digital ID platform

The business providers can examine the accuracy, genuineness and the valid of identification information and evidence of the customer including proving that the customer is the true owner of such information and evidence through digital ID platform as a replacement of customer verification or to be used for supporting the customer verification under Clause 4.2.2 and Clause 4.2.3. In addition, the business providers shall comply with the Electronic Transactions Development Agency (ETDA)'s recommendation on ICT standard for electronic transactions Re: Digital Identity Guidelines for Thailand – Enrollment and Identity Proofing as well as other related guidelines.

In this regard, the business providers must perform customer verification, using criteria in accordance with the identity verification standard for not lower than the risk level of each type of product and e-Money service activation channel under Clause 4.2.2 and Clause 4.2.3, as the case may be.

4.2.5 Service activation and a future change in the type of e-Money service type by the customer.

For the business providers who have already applied the regulations on KYC in this Notification to the customer activating e-Money service or changing the type of e-Money service, and regularly updating the customer information to be accurate and up-to-date, when the customers activate the e-Money service or next time they change their type of e-Money service, the business providers may consider to perform customer authentication method. In this regard, such customer authentication method must be rigorous and able to prove the true customer, and consistent with the risk level of each type of product and e-Money service activation channel. An example is that the business providers may apply the technology of biometric comparison to perform identity authentication to prove the true customer.

4.3 Policies, measures on risk management and other related internal control procedures

The business providers must stipulate in writing the policies and measures on risk management relating to KYC as well as the internal control procedures with the approval from the board of directors or the top management. These policies and measures aim that the risk management will be appropriate, rigorous and consistent with each type of

product and e-Money service activation channel which starts from the KYC process to the termination of using e-Money service by the customer. They are also to prevent frauds in form of counterfeit or the use of other people's information to activate the service and make e-Money transactions, and to protect customer's personal data by stipulating policies, measures of risk management and the internal control procedures which must cover at least the following key points:

(1) Clear policies and practice guidelines on customer identification, customer verification and customer's authentication.

(2) Measures to prevent and monitor risk of possible frauds such as transaction credit limit, examination of customer authentication, providing continuous monitoring system of the suspicious transactions and frauds.

(3) Measures to manage the IT risks relating to customer identification, customer verification and customer authentication that are consistent with the risk level and impact of applying technology to e-Money service providing as well as the IT security measures that are consistent with the generally accepted universal standards.

(4) Policy and operation procedures in data governance that is appropriate, rigorous and up to standard by setting Data Classification Policy that is consistent with the forms and risks of service providing, covering personal data which include customers' biometric data in every related procedure from acquiring, keeping, accessing, transferring and destroying data in order to ensure the strict protection of the customers' personal data including biometric data.

(5) Clear risk management measures and internal control procedures to deal with the situations where the business providers fail to comply with the regulations on customer verification for e-Money service activation for payment of goods or services and funds transfer as stipulated in Clause 4.2.2 (2) and Clause 4.2.3; such as suspension in examining the status of smart ID card through electronic examination system of the government agencies.

(6) Risk assessment and management that may arise from using the services provided by other service providers or other persons for any implementation relating to KYC.

In this regard, the business providers must regularly review or adjust policies, measures and internal control procedures to be appropriate with the situation, and

must disseminate to and train staff or concerned personnel to also comply with such policies, measures and internal control procedures.

4.4 Keeping of identification information and evidence

The business providers must keep the information and evidence for identification and verification acquired in accordance with this Notification. They shall record the details of transactions relating to KYC process in the secure system or place since the starting of KYC process by keeping it for a period stipulated in the regulations of Anti-Money Laundering law. This is for the BOT or other persons in authority according to other laws to examine, or to be used as supporting evidence for investigation and prosecution of crimes, or for the internal monitoring and control of the business providers.

4.5 Performing customer's verification with other methods

4.5.1 In case where the business providers wish to apply other methods or implementations apart from Clause 4.2.2 (2) and Clause 4.2.3 to the KYC process of which the assurance level is equivalent to the regulations stipulated in this Notification, a request for permission shall be submitted to the BOT on a case by case basis together with the related document stipulated in the public guide. The BOT will complete the request consideration process within 30 working days from the date on which the document has been received accurately and completely. In consideration for approval, the BOT may also stipulate any additional conditions as deemed appropriate for compliance.

4.5.2 In case where the business providers wish to apply the new technology to perform customer verification and it is likely to develop further to become an infrastructure or common standard which is necessary to be tested with the joint cooperation among the financial service providers, such technology must first pass the test and prove successful according to the BOT's guideline for participation in the test and development of the innovative technology to support financial services (Regulatory Sandbox). In consideration for approval, the BOT may also stipulate any additional conditions as deemed appropriate for compliance.

4.6 Relaxation of compliance with the regulations

In case where the business providers fail to comply with the regulations stipulated in this Notification as deemed necessary or under special circumstances which may

cause an impact on the continuity of service or the reliability of the e-Money service, the business providers can submit a request for relaxation of compliance with such regulations, clarifying the reasons and necessity to the BOT in writing or by the electronic means. In this regard, the BOT may or may not grant permission or may prescribe any other additional conditions for compliance.

5. Transitional Provision

When this Notification is in effect, if any business providers are not able to comply with the regulations on KYC for e-Money service activation as prescribed in Clause 4.2.2 (2), Clause 4.2.3, Clause 4.2.5 or Clause 4.3, the business providers shall develop the system and proceed with such stipulations to be complete within 180 days from the effective date of this Notification without submission of request for relaxation to the BOT.

Nevertheless, such business providers must present to the BOT the clear operating plan in compliance with the regulations and shall report the progress of the operating plan to the BOT within 60 days from the effective date of this Notification; and after compliance with the stipulated regulations, notification to the BOT shall be made promptly in writing or by electronic means.

6. Effective Date

This Notification shall come into force as from the day following the date of its publication in the Government Gazette.

Announced on 13th March 2020

(Mr. Veerathai Santiprabhob)

Governor

Bank of Thailand

Payment Systems Policy Department

Tel: 0 2283 5036, 0 2356 7230