Unofficial Translation

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

Please refer to the Thai text for the official version.

Notification of the Bank of Thailand

No. FPG. 19/2562

Re: Regulations on Know Your Customer (KYC)

for deposit-account opening at financial institutions.

---

1. Rationale

Know-Your-Customer (KYC) process is a measure used to accurately know and verify the identity of a person, to prevent fraud from counterfeit or the use of other person's data in making financial transactions. It is also a preventive measure for Anti-Money Laundering, Combating Financing of Terrorism and Combating Proliferation Financing (AML/CFT/CPF). The deposit-account opening at financial institutions is a crucial transaction and is a beginning for a customer to start using financial services in financial institutions system, which then may be used as a money laundering channel and may cause damage to data and asset of account owners as well as the financial institution system. KYC process is therefore very important for the deposit-account opening, hence, the Bank of Thailand prescribes regulations on know your customer, comprising 2 crucial steps: (1) Identification and (2) Verification, to ensure that financial institutions have KYC process that is effective.

Nevertheless, problems in KYC process during deposit-account opening is still evident e.g. the use of a lost ID card of other persons to open a deposit account. Together with increasingly advanced technology and decreasing costs, financial institutions are moving towards adopting technology that is credible and internationally acceptable for their business operations, including verification-support technology such as biometric comparison technology that helps accurately verify customer identity in the process of deposit-account opening. This technology can also benefit financial institutions on digital front e.g. the use of biometric comparison technology for authentication before customers can access the service or conduct a transaction with financial institutions.

Given the above-mentioned fraud problems and changing environment, the Bank of Thailand deems it necessary to revise the regulations to promote continued trustworthiness and security in financial transactions within the Thai

financial system, with the considerations on public financial access and business extension on the digital frontier to ensure efficiency of the financial institutions system.

Upon this regulatory amendment, the Bank of Thailand repeals the Identification section which financial institutions need to comply with regulations under the laws on anti-money laundering to reduce duplications on regulatory compliance. For the Verification section, the Bank of Thailand sets out additional regulations to the currently effective regulations under the laws on anti-money laundering to enhance efficiency, as well as, to reflect risk sensitivity of identity verification of different types and channels of deposit-account opening. On this, guidelines are set for financial institutions to comply when verifying the accuracy, reality and up-to-date nature of identification data and documents, as well as verifying whether a person that wishes to open a deposit account is the same person as the one in the identification documents. This notification also gives general permission for financial institutions to use biometric comparison technology in different forms depending on technological advancement, in order to enhance verification efficiency. Financial institutions must comply with other regulations related to the use of technology e.g. regulations on the information technology risk oversight for financial institutions, and the Bank of Thailand guidelines on regulatory sandbox.

For subsequent deposit-account opening of financial institutions' existing customers who have already completed KYC process under this notification, financial institutions can follow the KYC process under this notification or may consider using other processes according to customer's risk level and account-opening channels used that is in line with financial institution's risk management. This is because financial institutions have already completed the KYC process during that customer's first deposit-account opening, but the financial institution must also have effective authentication methods and must verify that a customer who wishes to open a deposit account is truly that existing customer e.g. financial institutions may use biometric comparison technology for authentication to verify that customer.

2. Statutory Power

By virtue of Section 41 of the Financial Institution Business Act B.E. 2551 (2008), the Bank of Thailand hereby issues the Regulations on Know Your Customer (KYC) for deposit-account opening at financial institutions for financial institutions to comply with.

3. Scope of Application

This Notification shall apply to all financial institutions according to the law on financial institution business.

4. Repealed Notification and Circular

Once the Bank of Thailand Notification regarding regulation on know your customer for opening e-money account under the laws on payment system becomes effective, repeal the Bank of Thailand notification and circular as follows:

1) The Bank of Thailand notification No. FPG. 7/2559 Re: Regulations on Acceptance of Deposits or Money from Customers dated 6 July 2016.

2) The Bank of Thailand circular No. BOT.RPD(21) C. 1688/2559 Re: Relaxation on Smart Card Reader enforcement for customer verification for the acceptance of deposits or money from customers dated 27 December 2016.

For all regulations prescribed under the above Bank of Thailand notification and circular that are in conflict with this notification, follow this notification instead.

5. Content

5.1 Definition

In this Notification,

"Deposit-account opening" means account opening to accept deposits or money from the public by financial institutions, according to the laws on financial institution business which does not include e-money account opening by financial institutions according to the laws on payment system.

"Customer" means a natural person, a juristic person or a person with legal agreement whose relationship is made through deposit-account opening with financial institutions.

"Person with legal agreement" means a natural person or a juristic person who is in legal agreement to hold, use, dispose, and manage assets by any means for benefits of the other natural person or juristic person.

5.2 Principle

Financial institutions can provide deposit-account opening services both by face-to-face, which financial institutions provide service to customers in person e.g. deposit-account opening at financial institution's branches, and by non face-to-face, which customers open deposit accounts via electronic or digital channels such as deposit-account opening through Kiosk machine, internet banking or mobile banking. For both types of deposit-account opening, financial institutions must have KYC process which is a process where financial institutions know and verify customer identity in that the customer who wishes to open a deposit account is truly that customer, to prevent fraud from counterfeit or the use of other person's data in making transactions and to prevent money laundering.

KYC process comprises of 2 crucial steps: (1) Identification and (2) Verification; which must follow.

1) Financial institutions must ensure that customers identify themselves, and financial institutions must verify accuracy, reality and up-to-date nature of the identification data and documents from customers, as well as verify whether a person that wishes to open a deposit account is the same person as the one in the identification documents.

2) Financial institutions must manage risks appropriately and consistent with the risk of transactions and channels used in opening a deposit account. Since a non face-to-face KYC process may entail higher operational risk compared to face-to-face KYC process, financial institutions must have a more rigorous verification process, as well as other methods e.g. monitoring of customer's deposit account to enhance the efficiency of such risk management.

3) Financial institutions must give due consideration and manage information technology risk efficiently, consistent with the risk level and impacts of the use of technology in deposit-account opening and ensure that information security is consistent with information security standards of financial institutions which can be referenced to widely acceptable international standards. This is to reduce the potential damage that may occur upon financial institutions from adopting information technology in both face-to-face and non face-to-face deposit-account opening, thereby enhancing the efficiency of KYC process.

4) Financial institutions must give due consideration to KYC process by establish internal policy and operational procedure within financial institutions that is clear and in writing, as well as review appropriately and communicate to ensure that relevant staff or personnel understand, realize the importance, and comply with

financial institutions' internal policy and operational procedure, as well as regulations by the Bank of Thailand and other relevant regulators. Also, financial institutions must communicate, clarify and educate customers so that they realize, are cautious of and are prevented from being under fraud deposit-account opening by other persons.

5) Financial institutions cannot open deposit accounts for customers who conceal their real names or use anonyms or fake names. However, the names of deposit accounts can be commercial names or other names that customers have supporting documents from government agencies, government, or original affiliation such as school or hospital.

5.3 Regulations on Know-Your-Customer

Financial institutions can conduct KYC steps for deposit-account opening either by face-to-face or by non face-to-face, and must comply with regulations as follows.

5.3.1 Identification

Financial institutions must obtain identification data and documents that identify customer identity, and identification documents obtained must be in accordance with customer types under the laws on anti-money laundering. Such identification data and documents also include data and electronic documents according to the laws on electronic transactions.

5.3.2 Verification

Financial institutions must verify the accuracy, reality and up-to-date nature of identification data and documents received under 5.3.1, as well as verify, without negligence, that it truly is this customer. Financial institutions must establish an internal operational process that is effective and must be reviewed appropriately. Financial institutions must comply with verification regulation as follows.

(1) Verification by financial institutions themselves

(1.1) Face-to-Face verification

Under face-to-face verification, financial institutions are the one who verify the accuracy, reality and up-to-date nature of identification data and documents received from customer identification, as well as verify that it

truly is this customer or a person with final authorization from a juristic person (if any). Data used for verification must be obtained from credible sources e.g. in the case of using smart-card ID as an identification document, financial institutions must verify data from the smart card reader and also verify smart-card ID's current status from the electronic verification system provided by government agencies. In addition, financial institutions may consider adopting biometric comparison technology to enhance the efficiency of customer verification.

If financial institutions provide off-premise account-opening service which the verification of juristic persons or wealth management customers is carried out by the relationship manager (RM) with a prior relationship with such specific customers, financial institutions can regard such relationship manager as equivalent to verification by the smart card reader. However, financial institutions must establish written internal policy and procedure to ensure that such operation is appropriate and effective. Examples of internal policy and procedure are the verification process to ensure the accuracy, reality and up-to-date nature of identification data and documents provided by juristic person customers, wealth management customers and persons with final authorization from juristic persons (if any), and the risk management process such as internal control process, suspicious account monitoring process and data storage process.

(1.2) Non face-to-face verification

Under non face-to-face verification, financial institutions must verify the accuracy, reality and up-to-date nature of identification data and documents received from customer identification, as well as verify that it truly is this customer or a person with final authorization from a juristic person (if any). Data used for verification must be obtained from credible sources such as in the case of using smart-card ID as an identification document, financial institutions must verify data from the smart card reader and also verify smart-card ID's current status from the electronic verification system provided by government agencies. In addition, financial institutions must take a photo of a customer and use liveness detection and biometric comparison technology to ensure that it truly is this customer, in order to substitute for a face-to-face process. If the use of the above-mentioned liveness detection technology cannot observe customer's behavior, financial institutions must establish additional process or risk management guidelines to reduce fraud risk e.g. a customer is forced or deceived to open a deposit account.

In the event that financial institutions cannot comply with the verification regulation in 5.3.2 (1.1), e.g. customers do not have smart-card ID, or

such ID has defects, or the electronic verification system provided by government agencies is interrupted, or the verification regulation in 5.3.2 (1.2), e.g. the liveness detection technology is interrupted, financial institutions must establish additional internal written operational process to manage risk from such events.

(2) Verification by digital verification and authentication system

Financial institutions can verify the accuracy, reality and up-to-date nature of identification data and documents, as well as verify that it truly is this customer or a person with final authorization from a juristic person (if any) through the digital verification and identification system such as National Digital ID Platform (NDID Platform) to substitute the verification under 5.3.2 (1) or to support verification under 5.3.2 (1). Financial institutions shall comply with the Electronic Transactions Development Agency's recommendation on information and communication technology standard for electronic transactions on the digital identity guideline for Thailand re: Enrolment and identity proofing by the Electronic Transactions Development Agency.

Nevertheless, the verification through the above digital verification and authentication system must be at least as effective as the verification by financial institutions according to verification regulations in 5.3.2 (1).

5.3.3 Identification data and document storage

Financial institutions must keep identification data and documents, including images, photo and audio (if any), as well as transaction logs and transaction details related to KYC process in a secured system or places from the day that financial institutions start the KYC process and keep those data and documents for a period specified by regulations under the laws on anti-money laundering, in order that the Bank of Thailand or persons with relevant legal power can supervise or use as evidence in the investigation or legal proceedings or for benefits of financial institutions in monitoring, auditing and internal control.

In addition, financial institutions must establish policy and operational procedure on data governance that is appropriate, effective, and up to standards, with the data classification policy that is consistent with types and risks of the service, covered personal and biometric data in every relevant step from data input, storage, access, transfer, and disposal. Financial institutions must frequently review policy compliance to ensure that customers' personal data and biometric data are strictly protected.

5.3.4 Compliance with other relevant regulations

Financial institutions must have guidelines and measures to ensure that KYC system and process, for both face-to-face and non face-to-face, are strictly in compliance with other regulations, policy statement, and guidelines of the Bank of Thailand, such as regulations on information technology risk of financial institutions, regulations on banking channel of financial institutions, regulations on outsourcing of financial institutions, and regulations on market conduct.

Financial institutions must also comply with guidelines on the regulatory sandbox prescribed by the Bank of Thailand. Under the circumstance that financial institutions adopt new technology that may develop into infrastructure or central standard, which service providers need to conduct joint testing, or when relevant laws or regulations require a test in the regulatory sandbox prior to giving service to the public, financial institutions must conduct a test in the regulatory sandbox. However, when new technology is adopted but it is outside the scope of the regulatory sandbox, financial institutions may arrange for a test within their own sandbox.

If a new technology related to customer's biometric data is adopted, financial institutions must give due consideration in order to ensure credibility to service users, and financial institutions shall discuss with the Bank of Thailand prior to the adoption.

Moreover, financial institutions must comply with other relevant laws, such as laws on anti-money laundering, laws on electronic transactions and laws on personal data protection.

5.4 Subsequent deposit-account opening of financial institutions' existing customers

Financial institutions can use the KYC process according to the regulation under this notification for the subsequent deposit-account opening of existing customers who already have deposit accounts with such financial institution and has completed the KYC process under this notification, or financial institutions may consider other processes according to that customer's risk level and service channel used that follows financial institutions' risk management. This is because financial institutions have already completed the KYC process during that customer's first deposit-account opening, but financial institutions must have effective authentication methods and must verify that a customer who wishes to open a

deposit account is truly that existing customer e.g. financial institutions may use biometric comparison technology for authentication to verify that customer.

5.5 Submission for the approval to the Bank of Thailand on a case-by-case basis

If financial institutions wish to opt for other KYC process or operation for deposit-account opening other than the regulations prescribed by the Bank of Thailand, as well as in the case that financial institutions cannot comply with regulations the Bank of Thailand prescribe in this notification, financial institutions shall submit for the Bank of Thailand approval as set out in the public guide, together with relevant documents. The Bank of Thailand will complete the consideration process within 30 working days from the day that all documents are correctly and comprehensively delivered, and may take comments of financial institution examiners into consideration, as well as set additional conditions for financial institutions to comply with where appropriate.

In considering the submission for the approval, the Bank of Thailand will consider based on principles of promoting efficiency of the financial institution system and enhancing micro-prudential stability including management system with due consideration and good risk management, fairness and consumer protection. The procedure or operation under the submission for the approval must (1) employ process or technology that is up to standards or widely acceptable with effective verification results (2) have a good risk management and internal control especially on customer data, and (3) comply with regulations under other laws such as laws on anti-money laundering.

5.6 Additional conditions, amendment, deferment or suspension of service

The Bank of Thailand may consider prescribing additional conditions, order to amend, defer, or suspend all or some of the operation should it is found that financial institutions do not comply with or contravene regulations prescribed by the Bank of Thailand within this notification or in other case that the Bank of Thailand deems that financial institutions' operation may impact public safety and the well-being or stability of financial institution or financial institution system.

5.7 Transitional provision

Once this notification becomes effective, if financial institutions cannot comply with regulation in 5.3.2 (1.1) or cannot specify the written internal operational process for the event that financial institutions cannot comply with verification standard, financial institutions shall complete the system development and comply with such guideline within 180 days from the date this notification becomes effective without the need to submit to the Bank of Thailand for relaxation.

However, financial institutions must submit the plan to comply with the above regulation and must submit a progress report to the Bank of Thailand within 60 days from the date this notification becomes effective.

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 23rd August 2019

(Mr.Veerathai Santiprabhob)
Governor
Bank of Thailand

Regulatory Policy Department
Telephone 0 2283 6876, 0 2356 7686