Unofficial Translation

This translation is for the convenience of those unfamiliar with the Thai language. Please refer to the Thai text for the official version.

Notification of the Bank of Thailand

No. FPG. 12/2564

Re. Regulations on Specialized Financial Institution's services through telephone and digital channels

1. Rationale

There have been significant improvements in the service provision channels of Specialized Financial Institutions (SFIs) over the years. Such channels have expanded on the back of technological advances, allowing SFIs to fulfill their mandates in a more efficient and effective manner. These developments, which partly reflect a need to meet changing customers' demand and behaviors, have increased access to and convenience in receiving financial services for end-customers.

Previously, the Bank of Thailand has issued regulations on SFIs' branch establishments, and regulations on SFIs' Business Facilitator Supervision. Covering significant service provision channels, including physical branches, digital branches, exchange offices, off-site operations, and financial service provision through business facilitators, these regulations aim to support SFIs in providing services to their target customer groups in accordance with the SFIs' mandates set out in the Establishment Act, and by the Ministry of Finance, and to ensure appropriate risk management.

Recognizing the growing importance of telephone and digital channels which have greatly advanced in recent years, the Bank of Thailand issues this Notification under the scope of the Establishment Act to set out additional regulations for SFIs with the aim of ensuring sound risk management and fair consumer treatment and protection.

2. Statutory Power

By virtue of Section 120/1 of the Financial Institution Business Act B.E. 2551 (2008), and the following amendments, the Bank of Thailand, with approval from the Minister of Finance, hereby issues Regulation on Specialized Financial Institutions' services through telephone and digital channels. SFIs shall comply with the regulation set out in this Notification.

3. Scope of Application

This Notification shall apply to the Government Savings Bank, Bank for Agriculture and Agricultural Cooperatives, Government Housing Bank, Small and Medium Enterprise Development Bank of Thailand, Export-Import Bank of Thailand, Islamic Bank of Thailand, and Thai Credit Guarantee Corporation.

4. Content

4.1 Definition

In this Notification,

"Specialized Financial Institutions" mean the state-owned financial institutions established under a specific establishment act, namely, Government Savings Bank, Bank for Agriculture and Agricultural Cooperatives, Government Housing Bank, Small and Medium Enterprises Development Bank of Thailand, Export-Import Bank of Thailand, and Thai Credit Guarantee Corporation.

"telephone channel" means a service provision channel through automatic telephone systems whereby customers receive services through menu-based functions set up by a particular SFI or its partner, or through interactive voice response (IVR) systems that allow customers to conduct financial transactions, as well as through other forms that go through the SFI's centralized systems that result in financial transactions i.e. through the SFI's call center. In addition, this also includes service provision that does not result in financial transactions, and service provision related to information and news dissemination.

"digital channel" means a service provision channel through internet banking and mobile banking.

"internet banking" means service provision through communication network or internet where customers use URL Website to access services through their electronic devices such as computers and mobile devices.

"mobile banking" means a service provision through a mobile banking application which is installed in a mobile device such as mobile phone and tablet.

"committee" means a committee of the relevant Specialized Financial Institution.

4.2 Principle

Providing services through telephone and digital channels is important for promoting greater access to financial services by SFIs in accordance with their mandate(s). In this respect, while the scope of SFIs' transactions is governed by the Establishment Act, the Bank of Thailand, as a regulator, releases regulations to ensure that the SFIs have a safe and sound risk management framework, as well as appropriately treat and protect their customers.

4.3 Conditions on service provision through telephone and digital channels

Providing services through telephone and digital channels may pose risks that have implications for the relevant SFI's ability to provide services, especially in the case of adopting a new technology for the first time or when existing underlying technologies change. In this respect, the SFI must ensure that its information technology system is up to standard and be approved by the Bank of Thailand prior to using such channel. To submit a request for approval, the SFI must abide by the Notification of the Bank of Thailand No. FPG. 19/2560 Re. Regulations on Financial Institutions' Information Technology Risk Supervision which was dated on 20 December 2017, until the Bank of Thailand issues a new regulation specifically on SFIs' Information Technology Risk Supervision.

In addition, the Bank of Thailand sets forth the following conditions on SFIs' service provision through telephone and digital channels (overview provided in Attachment 1).

4.3.1 Telephone channel

(1) To provide services that result in financial transactions, such as opening new deposit account, payment service, an SFI shall submit a request for approval to the Bank of Thailand as specified in Clause 4.5.1 before providing services in accordance with the public manual.

(2) To provide services that do not result in financial transactions, including providing information such as giving advice, responding to inquiries, activation and suspension of debit cards, and responding to credit card statement inquiries, an SFI can provide such services without requesting approval from the Bank of Thailand.

4.3.2 Digital channel

(1) To provide services, whether resulting in or not resulting in financial transactions, such as money transfer, payment service, opening new deposit account, providing loan-related services, debit card activation and suspension etc., an SFI shall meet the following requirements.

(1.1) First-time service provision

An SFI that wishes to 1) provide such services for the first-time, or 2) provide services on an additional channel(s) on top of its existing one(s), shall submit a request for approval to the Bank of Thailand as specified in Clause 4.5.1 prior to providing services in accordance with the public manual.

(1.2) Changing the service provision models

An SFI shall notify the Bank of Thailand 15 days in advance prior to providing services in case of adding, cancelling, or changing their service model that has been previously approved by the Bank of Thailand, as specified in the public manual. In this case, the Bank of Thailand may impose additional conditions for the SFI to comply with as deemed appropriate.

(2) To provide information dissemination services related to its products or services such as procedures for applying for a loan, transaction documents, and any important conditions, an SFI may provide such services without being granted approval from the Bank of Thailand.

To provide services through telephone and digital channels, an SFI shall comply with other related laws such as payment system laws, personal data protection laws, and guidelines on testing and developing innovations using new technologies to support financial services (Regulatory Sandbox).

4.4 Regulations on service provision through telephone and digital channels

4.4.1 Roles, duties and responsibilities of the relevant committee, and policy setting on service provision through telephone and digital channels

(1) Roles, duties and responsibilities of the relevant committee

(1.1) Approve policies and strategies of the SFI in providing services through telephone and digital channels that are consistent with its mandate(s), and monitor the implementation of such policies in setting up the relevant processes for service provision, risk management, and customer treatment and protection. In addition, the committee must assign the executives or staff responsibilities for implementing such policies and procedures, in addition to communicating their essence thoroughly to the relevant executives and staffs by providing a handbook or guideline on best practices for providing services through telephone and digital channels.

(1.2) Review and evaluate the effectiveness of policies and procedures at least once a year, and each time there is any change that significantly affects the services being provided, such as due to a change in the underlying technology or a change in the business strategy on service provision through telephone and digital channels.

(2) Setting policies on service provision through telephone and digital channels

An SFI shall set policies on service provision through telephone and digital channels. Those policies must be approved by the committee and the content must cover at least the following details.

(2.1) Responsibilities of executives and staff involved in providing services.

(2.2) Guidelines on risk management related to service provision that are consistent with the overall risk management policies of the organization and are in accordance with Clause 4.4.2.

(2.3) Guidelines on the treatment and protection of customers that are consistent with the organization's overall policies on fairness in service provision, and are in accordance with Clause 4.4.3.

(2.4) Guidelines for monitoring compliance with policies on service provision through telephone and digital channels approved by the committee, as well as for monitoring compliance with approved policies on service provision procedures, risk management, and customer treatment and protection.

(2.5) Guidelines for performance reporting to the committee, the subcommittee(s), and executives, such as on service efficiency and abnormal circumstances that pose risk to the SFI and its customers.

4.4.2 Risk management

(1) General regulations

An SFI must have sound risk management, which is consistent with its risk management framework and which is a part of a service provision policy approved by its committee. The SFI shall comply with the following requirements on risk management for telephone and digital channels.

(1.1) The SFI must have thorough knowledge and understanding of risks that may arise from providing services through telephone and digital channels, such as operational risk, strategic risk, reputational risk, and information technology risk.

(1.2) Processes, operations, and systems that are established by the SFI must be able to indicate, evaluate, and control risks appropriately, in addition to being able to cover all related risks, especially operational risk such as system interruptions from human errors and internal and external frauds, as well as strategic and reputational risks. In addition, the SFI must train and supervise its staff to strictly perform according to the set procedures. The SFI must implement processes and procedures in practice, regularly monitor risks, and reflect on issues that come up during service provision to further improve the relevant processes, systems, and internal controls.

(1.3) Risk management guidelines should at least cover the following issues.

(1.3.1) Internal controls

The SFI must have appropriate systems and internal controls that are effective at reducing risk arising from its service provision through telephone and digital channels. Such systems and controls must be consistent with policies and strategies approved by the committee. In this regard, the SFI must communicate to the relevant stakeholders about its roles and responsibilities, closely monitor compliance with the established systems and controls, and report to the committee or executives about any detected flaws in the systems and controls, with the aim of making them more effective and efficient.

(1.3.2) Service safety

The SFI must have guidelines and appropriate security measures for providing services - both the security of the SFI's system and customers' personal data – that are consistent with the risk management guidelines for providing services through telephone and digital channels. The aims are to ensure that customers' personal data are protected and to prevent any damage that may affect the customers and the SFI.

(1.3.3) Readiness and continuity of services

The SFI must have measures to monitor and control the readiness of providing services by having in place a system capacity plan and a business continuity plan (BCP) in the case where there are abnormal circumstances, so as to ensure smooth and uninterrupted provision of services. In addition, the SFI must have the necessary guidelines and preparations for the case where its service provision is interrupted, or it is unable to provide services as previously agreed with customers. The SFI shall comply with the Bank of Thailand's guidelines on business continuity management (BCM) and BCP for SFIs.

(2) Additional regulations

Services provided through the digital channel that result in financial transactions may have specific characteristics that pose risks to customers on a wide scale. As such, in addition to the general regulations specified in Clause 4.4.2 (1), the SFI shall comply with additional regulations on risk management for providing services that result in financial transactions through the digital channel as specified in Attachment 2.

4.4.3 Treatment and protection of customers

An SFI must comply with the Bank of Thailand's Notifications on Market Conduct and the additional regulations on customer protection as follows.

(1) General regulations

An SFI must comply with guidelines on customer treatment and protection that are approved by its committee. Such guidelines must cover details on responsible and fair treatment of customers and take into account customers' ability to access to services provided through each channel, and steps to ensure access to services by those requiring special assistance - such as customers with disabilities. In addition, the SFI must comply with the following general requirements on customer treatment and protection under telephone and digital channels.

(1.1) Providing knowledge and advice, and taking care of customers.

An SFI must have guidelines for providing knowledge and advice on service provision through telephone and digital channels, particularly on safe use of technologies, to increase customers' understanding. Additionally, the SFI must disclose important information relating to service provision to customers in a complete, accurate and undistorted manner, in order to provide customers with information necessary for informed decision-making. Furthermore, the SFI must have guidelines for problem-solving and dealing with complaints in order to ensure fair and effective treatment of its customers. Should there be any change or cancellation in its services, the SFI must also notify its customers through appropriate channels and establish a plan to take care of the affected customers.

(1.2) Service suspension

(1.2.1) In case of emergency or force majeure

An SFI must notify customers of any service suspension as soon as possible through appropriate channels and notify if there is a resumption of the relevant service(s) as soon as possible.

(1.2.2) In the case of a planned temporary service suspension, such as planned system maintenance, the SFI must notify its customers in advance, including information on the duration, through appropriate channels. To this end, the SFI must provide a channel/platform through which customers can contact for inquiries, reporting problems, or submitting complaints about services. In addition, if there is any fees or charges that affect the customers, the SFI must communicate such information to its customers clearly and completely.

(2) Additional supervision regulations

Since services provided through the digital channel that result in financial transactions may have specific characteristics that pose risks to customers on a wide scale, an SFI shall comply with the general regulation on consumer treatment and protection as specified in Clause 4.4.3 (1), in addition to additional regulations on customer treatment and protection, for service provision that results in financial transactions through a digital channel as specified in Attachment 2.

4.5 Obtaining approval and waiver from the Bank of Thailand

4.5.1 If an SFI wishes to provide services through a telephone channel as specified in Clause 4.3.1 (1) and a digital channel as specified in Clause 4.3.2 (1.1), the SFI shall submit a request for approval to the Bank of Thailand as specified in the public manual, together with relevant documents. The Bank of Thailand will consider the request within 60 days from the date the request is received and all relevant documents are verified to be complete and accurate. In considering such a request, the Bank of Thailand may impose additional conditions upon approval.

4.5.2 If there is any force majeure that causes non-compliance with this Notification, an SFI may request a waiver from the Bank of Thailand on a case-by-case basis, by demonstrating the rationale, necessity, and plan to comply with this Notification as specified in the public manual.

In considering such approval and waiver, the Bank of Thailand will take into account the relevant micro-prudential, macro-prudential, efficiency, governance, and fairness and customer protection factors.

4.6 Imposing additional conditions, and delay or suspension of service(s) or service provision channel(s)

If there is any non-compliance with this Notification, the Bank of Thailand may consider delaying, suspending, or withdrawing the SFI's service(s) or service channel(s) partially or wholly. In addition, the Bank of Thailand may impose additional conditions on a case-by-case basis as necessary.

4.7 Transitional provision

4.7.1 If an SFI provides services through telephone or digital channels prior to the effective date of this Notification, the SFI shall continue the relevant operation and must comply with this Notification.

4.7.2 If an SFI cannot comply with Clause 4.4 on the effective date of this Notification, the Bank of Thailand grants a general waiver. However, the SFI shall take actions necessary to ensure compliance within 120 days from the effective date of this Notification.

5. Effective Date

This Notification shall come into effect from 1 January 2022.

Announced on 4 October 2021

(Mr.Sethaput Suthiwartnarueput)

Govenor

Bank of Thailand

Regulatory Policy Department 1

Telephone 0 2283 6876

Attachment 1

Overview of conditions on providing services through telephone and digital channels

<table>
<tr><td colspan="4">Transaction scope in accordance with Establishment Act and under the Ministry of Finance's consideration</td></tr>
<tr><td colspan="4">The Bank of Thailand's scope of supervision focused on "risk management" and "customer treatment and protection"</td></tr>
<tr><td>Service provision conditions</td><td>Financial transaction services
such as money transferring, money receiving, and opening a new account</td><td>Non-financial transaction services
such as card activation and suspension, and statement request</td><td>Information provision services
such as knowledge sharing, advisory services, and inquiries</td></tr>
<tr><td colspan="4">SFIs' IT system must be approved by the Bank of Thailand and ready before going live. SFIs shall comply with the Notification of the Bank of Thailand No. FPG. 19/2560 Re. Regulations on Financial Institutions' Information Technology Risk Supervision, until the Bank of Thailand issues a specific regulation for SFIs</td></tr>
<tr><td>Telephone channel</td><td>Approval needed</td><td colspan="2">Able to provide services generally</td></tr>
<tr><td>Digital channel
(Internet & Mobile banking)</td><td colspan="2">Services that result in both financial and non-financial transactions
1. First-time service provision / addition of new channel: approval needed
2. Changing/cancelling service provision: notification needed</td><td>Able to provide services generally</td></tr>
<tr><td colspan="4">In addition, SFIs shall comply with other related laws such as Payment System laws, Personal Data Protection laws, and guidelines on testing and developing innovations using new technologies to support financial service provision (Regulatory Sandbox).</td></tr>
</table>

Attachment 2

Additional regulations on financial transaction service provision through a digital channel

Financial transaction service provision includes internet banking and mobile banking. An SFI providing such services shall comply with general regulations on risk management, customer treatment and protection, as well as regulations set out in this Attachment. In response to rapid technological advancements, an SFI may establish additional risk management processes or augment an existing ones to cover potential new risks appropriately, especially risks that affect customers.

In providing services through mobile banking, an SFI should follow the Bank of Thailand's Guiding Principles for Mobile Banking Security and adapt appropriately.

1. **Additional regulations on financial transaction service provision through a digital channel**

1.1 Risk management

An SFI must carefully manage risks related to service provision through a digital channel, particularly risks that may affect customers - including the registration process, service provision process, transaction execution process, and customers' information modification process - so as to ensure customers' confidence as well as their safe use of the SFI's services through the digital channel, as follows.

1.1.1 Application process

An SFI must have a comprehensive and secure protocol for managing the registration process, in order that minimize risk of impersonation that may result in frauds, covering at least the following aspects.

(1) An SFI must ensure thorough identification and verification of customers who register for services. In this process, at least two documents shall be used to minimize the risk of impersonation that may result in fraudulent activities. Examples of such documents include national ID number, account number, ATM

number and password, and email or mobile number with one-time password (OTP) that is sent to the customer's email or mobile number, where such an email or number is used to register for the SFI's internet banking or mobile banking service(s).

(2) Controlling of user account creation to prevent the use of duplicate accounts that may result in fraudulent outcomes.

(3) Secure and commonly accepted authentication process for accessing services, such as setting password to verify identity. A password should have minimum length, be difficult to guess, and set at a regular frequency. The authentication process may also utilize biometric data which are difficult to forge, such as fingerprint, face, and iris.

(4) In providing services through mobile banking, an SFI should look for and handle fake applications on other trustworthy and credible e-marketplaces, to mitigate the risk that their customers will download and install such applications.

1.1.2 Accessing the services

An SFI must have a comprehensive and secure process in controlling access to services, to mitigate risk of frauds and human errors. Such a process shall cover at least the following aspects.

(1) Customers must verify identity each time before logging into a system, except for low-risk transactions and when there is a pre-agreement with the customers.

(2) Controlling the display of customers' sensitive information that is used in the verification process, such as masking of customers' password or PIN code.

(3) Restarting the verification process if there is an interruption during verification.

(4) Notifying customers when there is a mismatch in the information used for verification. The system should not provide information on which

specific information is associated with the mismatch. In addition, when the number of attempts exceeds a certain number, the SFI must temporarily suspend the related account and provide information on how to reopen the suspended account, such as contacting a call center or branches. Furthermore, the SFI must have a verification process for cancelling the suspension of an account.

1.1.3 Making transactions

An SFI must have a process for ensuring safety while customers are making transactions, covering at least the following aspects.

(1) Controlling customers' authentication using appropriate methods according to the level of risk associated with the transactions.

(2) Controlling the display of customer's sensitive information that is shown on the screen, such as masking account number, except when otherwise pre-agreed with customers.

(3) Sending an error message to a customer(s) when there is a system error during services provision or transaction execution. This message must not contain information about the system's internal operations such as system design.

(4) Automatically terminate a session if there is no transaction made within a specified timeframe (session timeout), in order to prevent another person from using a customer's account without permission, such as if there is no transaction made for more than 3 minutes.

(5) Restarting the verification process if there is an interruption or a session timeout.

(6) Immediately notify the result of each completed and non-completed transaction to the customer according to the SFI's established protocol, such as sending an electronic message except where there is a force majeure or otherwise a pre-made agreement with the customer.

(7) Collecting and displaying transaction history so that customers can verify accuracy or request information on past transactions.

1.1.4 Changing customers' information

An SFI must have a comprehensive and secure control process for changing customers' information in order to reduce the risk of impersonation that may lead to fraudulent activities, as well as to reduce the risk of data leakage. Such a process must cover at least the following.

(1) Strict customers' identity verification if there is a request for changing customers' information.

(2) Sending a notification to customers' registered mobile number or email every time their information, such as email and favorite account, is edited.

(3) Collecting and displaying a customers' data amendment history so that customers can verify and request information on past changes and edits.

1.2 Customer treatment and protection

An SFI must have a process for providing information, knowledge, and taking care of customers so that customers will comprehensive information to make a decision, and can use the SFI's service(s) through a digital channel safely. Such a process must cover at least the following.

1.2.1 In case where there is an error during service provision or transaction execution

If there is an error during service provision or transaction execution, such as an interruption in the system that causes an unsuccessful money transfer, the SFI must display an error message indicating that there is an error and the transaction is not completed.

1.2.2 In case where other businesses' products or services are displayed

In the case where an SFI allows other businesses to display their products or services on the SFI' digital platform, the SFI must have a process in place to ensure that customers know that such products or services are not those of the SFI. The SFI shall also clearly specify the scope of its responsibilities.

If an SFI connects their digital platform with other businesses' digital platform, the SFI must create a clear pop-up message in their digital platform to clearly inform customers that they are leaving the SFI's digital platform to other businesses' digital platform.

1.2.3 In case of interruption or threat to the service provision system

In the case where there is an interruption or a threat to the service provision system that may limit customers' ability to access services through a digital channel or cause damage to customers, an SFI must communicate quickly to the customers and the media about related problems and resolutions in order not to cause any misunderstanding or panic.

1.2.4 Alerting of electronic scam behaviors

An SFI must have a process for alerting customers of electronic scam behaviors such as creating a website to duplicate the website of the SFI.

1.2.5 Educating and advising customers to ensure safe use of the digital channel and security of electronic device

An SFI must have a process for giving knowledge and advising customers to safely use services through its digital channel.

Examples: Notifying and advising customers on

- Storing authentication information in a secure place and not to entrust such information to other individuals.
- Verifying that the SFI's digital channel is not a duplicated channel before making transactions, especially in case of the SFI' digital channel being connected to websites, applications, or other channels.
- Making transactions carefully by not making transactions at unsecure locations (e.g. where other people can see the customer' important information that is used for accessing services or making transactions).
- Logging out from the system every time after completing transactions so that other people cannot get access to the customer' information without approval.
- Not making transactions through devices that have been modified.
- Checking the accuracy of the customer' transactions and information regularly. If there are any inaccurate transactions, customers shall notify the SFI immediately.
- Controlling access to personal information through an electronics device by setting a password, and setting auto-lock.
- Installing tools or security technology in a device such as Anti-Virus, and always updating relevant operating systems.
- Not leaving an electronic device unattended while making transactions.
- Installing or using programs from reliable sources, and avoiding visits to suspicious websites or opening suspicious e-mails.
- In case of getting a new mobile phone, the customer must re-install the mobile banking application or contact the call center to confirm application activation.

1.2.6 Service cancellation

An SFI must provide channels/platforms, such as a website or a call center, through which customers can easily contact to cancel services, especially in the case of loss of a device in which mobile banking is installed.