Bank of Thailand Notification
No. SorNorChor. 1 /2561
Re: Regulations on Supervision for System Operator of the Highly Important Payment Systems

---

1. Rationale

Highly important payment system is a principal infrastructure of the country. It is a payment system handling large value fund transfers or being used for clearing or settlement, which provides a linkage between a central bank and business providers of various payment systems who are members of the system. It also has a linkage (interdependencies) with systems used for trading securities in the stock exchange and other relevant systems; in order to facilitate convenient, fast and efficient processing of financial transactions, to support economic activities, and to maintain financial stability of the country. Any disruption of its operations would be likely to affect public interests, public confidence, or security and stability of the payment systems.

The Bank of Thailand therefore prescribed the regulations on supervision for system operator of the highly important payment systems, by applying principles from international standards. There are regulations relating to protection of payment finality, and procedures for the case that a member has been under a receivership order or has been adjudged bankrupt by the court; in order to ensure that there will be no impact on payment transactions in the highly important payment systems that have already been settled successfully. In addition, there are supervisions on governance, risk management and security, protection of members and public, and promotion of efficiency; which promote the highly important payment systems to be efficient, secure and safe, to have appropriate risk management, to continuously operate under normal and emergency conditions, as well as to reduce systemic risk; which lead to the stability of the payment systems and overall financial systems.

2. Statutory Power

By virtue of Section 7 of the Payment Systems Act B.E. 2560 (2017), the Bank of Thailand hereby issues the regulations on supervision for system operator of the highly important payment systems.

3. Scope of Application

This Notification shall apply to system operators undertaking the highly important payment systems according to the law governing payment systems.

4. Content

4.1 Definition

In this Notification,

"Highly Important Payment Systems" means the payment systems that the BOT establishes and operates according to the law governing the Bank of Thailand, or any other payment systems prescribed by the Minister in a notification with the advice of the BOT according to the law governing payment systems.

"System operator" means system operator who undertakes the highly important payment systems.

"Member" means a user who agrees to be bound by the rules for using services of the highly important payment systems.

"BOT" means the Bank of Thailand under the law governing the Bank of Thailand.

"Board" means the Payment Systems Committee according to the law governing the Bank of Thailand, or a board of the system operator of the Highly Important Payment Systems as prescribed by the Minister in a notification.

4.2 Regulations on supervision

The system operator shall comply with regulations, procedures and conditions as follows:

4.2.1 Payment finality

Fund transfer or settlement transactions that has been submitted to the highly important payment systems shall be considered final when the system operator deducted the fund from the sending member's account and deposited it into the receiving member's account according to rules of the systems specified by the system operator. The system operator, members or relevant stakeholders shall not be able to revoke, reverse or modify the transactions.

In this regard, the system operator shall prescribe rules, conditions and operating procedures relating to fund transfer or settlement regarding the finality of fund transfer or settlement by specifying processes, time period for payment and the point at which finality of fund transfer or settlement takes place (point of finality); and have a clear practice for such regulation.

4.2.2 Procedures for the case that a member has been under a receivership order or has been adjudged bankrupt by the court

(1) Establish procedures and practice guidelines for handling the case that a member has been under a receivership order or has been adjudged bankrupt by the court, including practices for coordination between members and relevant stakeholders such as regulators and operators of the connected systems (interdependencies); in order to proceed with a temporary suspension of services or terminate services providing to such member promptly, which reduce risks that potentially cause damages and liquidity problems.

(2) Have in place the testing of procedures and practice guidelines together with members and relevant stakeholders, including review procedures and practice guidelines for the case that a member has been under a receivership order or has been adjudged bankrupt by the court at least once a year or when there is a change that significantly affects the specified procedures and practice guidelines.

4.2.3 Governance

(1) Internal control

(1.1) Have in place the organizational structure that promotes risk management and internal control which is in line with a principle of three lines of defence by clearly separating the assignment of duties, responsibilities, line of commands, and reporting in accordance with functions of (1) operating the highly important payment systems (2) risk management and (3) audit; including have in place independent checks and balances especially for the audit function which must be independent from the function of operating the highly important payment systems and the function of risk management.

(1.2) Have in place the process for internal control which covers an inspection of irregular transactions to prevent risks arising from mistakes or fraud in the operation, or the risk management that is not sufficiently appropriate and cautious, or failure to comply with internal rules, practices, or orders of the system operator, or relevant laws.

(2) Reporting of operating performances and significant plans

Report of operating performances and significant plans relating to the highly important payment systems to the board regularly in order to monitor the operations such as plans for changing core systems, mitigation or improvement for major risks, target setting for providing services, and system availability reporting.

4.2.4 Risk management and security

The system operator shall comply with the regulations under the BOT's notification regarding policies and measures on security of Information Technology (IT) systems, and additional regulations as follows:

(1) Policy and measures on risk management

Establish risk management policy and measures in various aspects relating to the systems such as credit risk, liquidity risk, operational risk as well as information technology risk and cyber threats, including identify risk appetite which arises from systems of the system operator, members and connected systems (interdependencies).

In this regard, the risk management policy and measures must be approved by the board, and have in place a review of risk management policy and measures at least once a year.

(2) Policy and measures on security of Information Technology (IT) systems

Have in place an audit of the IT system security conducted by an external auditor at least once a year, and submit a copy of the audit findings report to the BOT in writing or by the defined electronic means within 45 days from the date on which the audit is completed. The audit scope shall include vulnerability assessment and penetration test in order to test the efficiency of security technology.

For the IT audit, the system operator shall select an external auditor who is independent and has knowledges and experiences in examining and assessing IT risks.

In the case that the system operator cannot perform the audit of the IT system security according to the prescribed regulation due to necessity or extraordinary circumstances, the system operator can submit a request for relaxation on compliance with such regulation together with reasons and necessity to the BOT in writing or by the defined electronic means, which the BOT may or may not grant an extension of time period, or may prescribe additional conditions for compliance.

(3) Business Continuity Management (BCM) and Business Continuity Plan (BCP)

(3.1) Establish policy on Business Continuity Management (BCM) along with the analysis and assessment of the impact of the system disruption, and prepare a Business Continuity Plan (BCP).

(3.2) Have in place the testing and review of the Business Continuity Plan (BCP) together with members and relevant stakeholders at least once a year and upon every significant change of the systems.

(4) Critical service provider

In the case of using services provided by other service providers or third parties for the operation on behalf of itself in the IT system functions and other functions that have a significant impact in providing services (critical service provider), the system operator shall take actions as follows:

(4.1) Establish outsourcing policy covering the risk management for outsourcing, security and confidentiality of systems and information, integrity of systems and information, and availability of the IT systems.

(4.2) Have in place the assessment and management on potential risks which should cover the protection of confidentiality and data privacy, and risks arising from critical service providers (interdependency risk) which may cause difficulty in changing or terminating the services used (vendor lock-in), including risks arising from concentrations of critical resources (concentration risk) especially for the case that critical service providers provide services to many users.

(4.3) Have in place a Business Continuity Plan (BCP) that covers the outsourcing activities, in order to handle the case of problems or unusual incidents from outsourcing activities and to reduce any potential impacts.

4.2.5 Protection of members and public

(1) Establish and disclose the service agreement

Establish a service agreement in a written form, and disclose the clear and up-to-date agreement to the members; which must at least consist of the followings:

(1.1) Rights, duties and liabilities of the system operators and members for both normal and emergency conditions.

(1.2) Rules, conditions and procedures in providing services.

(1.3) Financial risk or other risks that might arise from using the services (if any) in order to enable the members to assess any relevant risks arising from the use of services.

In this regard, the system operators have a duty to monitor to ensure that the members comply with the defined rules and conditions. There shall be in place the procedures for dealing with members who violate or fail to comply with the defined rules and conditions. In the case that the system operators make any changes to such rules which cause disadvantages to the members, the system operators must notify the members in advance no less than 30 days before that change comes into effect, by notifying details of such changes via electronic channel, or in writing, or by any other methods that enable the members to be informed.

(2) Notify other members in the case of suspension or termination of services providing to a member

(2.1) In the case of temporary suspension or termination of services providing to a member, the business system operator shall notify other members immediately.

(2.2) In the case that a member resign from the system, the system operator shall notify other members in advance no less than 15 days through electronic channel, or in writing, or by any other methods that enable the members to be informed.

(3) Protect data privacy of members

(3.1) Establish policy to protect data privacy of the members, determination of the level of confidentiality for data access, and identification of persons

who have access rights to such data; and arrange the systems for data storage that is accurate and reliable; and prevent an unauthorized person who has no relevant authority from accessing to or modifying the data maintained.

(3.2) Protect the members' confidentiality and data privacy by not disclosing such information during the course of services and after ceasing to provide services, except for the following cases:

(3.2.1) Disclosure upon obtaining consent from members in a written form or by any other electronic means as specified by the system operator.

(3.2.2) Disclosure for the purpose of investigation or trial.

(3.2.3) Disclosure to the auditor of the system operator.

(3.2.4) Disclosure for the purpose of policy formulation and oversight of the payment systems of the BOT.

(3.2.5) Disclosure for the purpose of compliance with laws.

(4) Fee disclosure

(4.1) Disclose details of the fees being charged to the members including the discount policies (if any) to enable the members and public to be informed.

In this regard, in setting the fees, the system operators must also consider fairness to the members.

(4.2) In the case of changing fees, the system operators must notify the members in advance no less than 30 days before that change comes into effect by notifying the details of such change via electronic channel, or in writing, or by any other methods that enable the members to be informed.

4.2.6 Promotion of efficiency

(1) Access and exit regime

(1.1) Establish objectives, rules, conditions, procedures, and fees or expenses relating to the access and exit regime clearly in writing; by considering the principles of fair and open access, and disclosing them to the members and public.

(1.2) Have in place risk assessment and related impact analysis relating to the acceptance of new members to access the systems such as financial position and readiness to connect with and use the systems; in order to ensure that the acceptance of new members will not pose risks and impacts to existing members in using the services.

(1.3) Disclose the up-to-date name list of the members so that the members and public are informed such as posting on the website of the system operator.

(2) Undertaking business with efficiency and effectiveness

(2.1) Define targets for providing services which are assessable and measureable such as system availability, and have in place the monitoring and evaluation, including report the results to the board regularly, as well as disclose the important operating performances in providing services according to the targets to the members.

(2.2) Establish mechanisms to survey and receive feedback from the members relating to important services regularly such as scope of services, functions of system usages, or choices of adoption of technology or procedures, etc. in order to develop and improve the systems to meet the members' needs and keep up to date for the rapid change of the technology.

5. Effective Date

This Notification shall come into effect from 16 April 2018.

Announced on 16th April 2018

(Mrs. Ruchukorn Siriyodhin)
Deputy Governor, Financial Institutions Stability
Governor for
Bank of Thailand

Payment Systems Policy Department
Tel. 0 2283 5095, 0 2283 5137