G.N. 5152

PAYMENT SYSTEMS AND STORED VALUE FACILITIES ORDINANCE

Guideline on Oversight of Designated Retail Payment Systems

A Guideline issued by the Monetary Authority under Section 54(1A)(a)

September 2020

Structure

1. INTRODUCTION

1.1. Purpose

1.1.1. The Monetary Authority (MA)[1] is responsible for designating important retail payment systems (RPSs) and overseeing their operation pursuant to the Payment Systems and Stored Value Facilities Ordinance (PSSVFO).

1.1.2. The Guideline on Oversight of Designated Retail Payment Systems (the Guideline) is issued by the MA pursuant to section 54(1A)(a) of the PSSVFO to explain the MA's interpretation of some of the oversight requirements under the PSSVFO relating to designated RPSs so as to assist system operators (SOs) or settlement institutions (SIs) of designated RPSs in understanding and complying with such requirements.

1.1.3. Pursuant to section 7(1)(a) of the PSSVFO, every SO and SI of a designated RPS shall ensure that the operations of the system are conducted in a safe and efficient manner calculated to minimize the likelihood of any disruption to the functioning of the system, with section 8(1) and (2) of the PSSVFO setting out some of the matters that are considered as relating to the "safety" and "efficiency" of the system respectively. Further, section 7(1)(b) and (c) of the PSSVFO stipulate that the SO and SI of a designated RPS shall ensure that the system has in place operating rules that comply with the relevant requirements under the PSSVFO and adequate arrangements to monitor and enforce compliance with the operating rules of the system. The Guideline sets out the high-level principles that the MA adopts in assessing the safety and efficiency of a designated RPS, its operating rules and compliance monitoring arrangements for the purpose of complying with the relevant statutory requirements. For the avoidance of doubt, the Guideline does not apply to clearing and settlement systems designated under the PSSVFO.

[1] The Monetary Authority is the public officer appointed by the Financial Secretary under section 5A(1) of the Exchange Fund Ordinance. The powers under the Payment Systems and Stored Value Facilities Ordinance are vested in the Monetary Authority. The office of the Monetary Authority is known as the "Hong Kong Monetary Authority" (HKMA).

1.1.4. The Guideline is not intended to be a comprehensive guide to the requirements relating to designated RPSs under the PSSVFO. SOs and SIs of designated RPSs should familiarise themselves with the PSSVFO and comply with all obligations imposed on them in relation to designated RPSs, and ensure that the requirements applying to designated RPSs are met on a continuing basis. The MA will monitor compliance with the PSSVFO requirements during his ongoing oversight of the designated RPSs.

1.1.5. The proper functioning of a designated RPS is material to the monetary or financial stability of Hong Kong or the functioning of Hong Kong as an international financial centre, or is relevant to matters of significant public interest. The HKMA therefore expects prompt reporting by SOs and SIs of designated RPSs of any potential inability to meet applicable statutory and/or regulatory requirements, or any breach of the operating rules of a designated RPS which may have a material impact on the safety or efficiency of the system.

1.1.6. The MA may update the Guideline and/or issue further guidance relating to designated RPSs as and when necessary.

1.2. Terminology

1.2.1. Unless otherwise defined in the Guideline, interpretation of terms used in the Guideline shall follow the definitions of those terms in the PSSVFO where applicable. Certain terms are summarized below for ease of reference[2]:

(a) "retail payment system" means a system or arrangement for the transfer, clearing or settlement of payment obligations relating to retail activities (whether the activities take place in Hong Kong or elsewhere), principally by individuals, that involve purchases or payments; and includes related instruments and procedures;

(b) "designated retail payment system" means an RPS designated under

[2] To facilitate understanding, the meanings in respect of certain terms defined in the PSSVFO are recast, elaborated or simplified.

section 4(1) of the PSSVFO;

(c) "system operator" means any person who, for the purposes of the operating rules of an RPS, is responsible for the operation of the transfer, clearing or settlement functions of the system, or any other related functions;

(d) "settlement institution" means a person providing services for the settlement of any payment obligation relating to retail activities for the purposes of the operating rules of an RPS;

(e) "participant" means a person who for the time being is a party to the arrangement by which an RPS is established; and

(f) "operating rules" means the rules or terms that govern the operation, use or functioning of an RPS.

2. SAFETY REQUIREMENTS

2.1. Introduction

2.1.1. Under section 8(1) of the PSSVFO, reference to the safety of an RPS includes in particular any matter relating to (a) the extent to which the operating rules of the system provide for certainty as to the circumstances under which transfer orders effected through the system are to be regarded as settled for the purposes of the system; (b) the reliability and robustness of operation of the system; (c) access control over the system; (d) the integrity of, and access control over, the information held within the system; (e) the risk management and control procedures relating to the operation of the system; (f) the soundness of the system, including financial soundness; (g) the services provided to the system by the infrastructure associated with the system; and (h) the criteria regarding the safety of the system prescribed for the purposes of section 8(1) of the PSSVFO.

2.1.2. This Chapter sets out the high-level principles that the MA adopts in assessing whether the operations of a designated RPS are conducted in a safe manner calculated to minimize the likelihood of disruption to the functioning of the system, taking into account the matters stipulated in section 8(1) of the PSSVFO.

2.2. Legal basis

2.2.1. A designated RPS should have a well-founded, clear and enforceable legal basis which provides for a high degree of certainty for its activities. There should be clear rules, procedures and contracts that govern the establishment and operation of the system, define the rights and obligations of the system, and its participants and other relevant parties, including where relevant, specifying the requirements on the system's participants' customers which shall be enforced via contractual arrangements between such participants and their customers. Such rules, procedures and contracts should be consistent with relevant laws and regulations. A designated RPS conducting business in multiple jurisdictions should

identify and mitigate the risks arising from any potential conflict of laws across jurisdictions that may render the designated RPS unable to meet the requirements under the PSSVFO, including any applicable rules or regulations issued by the MA pursuant to the PSSVFO.

2.2.2. The SO and SI of a designated RPS should ensure that the system and its operations are in compliance with applicable laws and regulations, including but not limited to the PSSVFO and the Personal Data (Privacy) Ordinance.

2.3. Governance, risk management and control procedures

2.3.1. The SO and SI of a designated RPS should have in place governance arrangements that are clearly defined and transparent, and promote the safety and efficiency of the system. The governance arrangements should provide clear and direct lines of responsibility and accountability. Management information systems should be in place to support effective management oversight of the designated RPS. The board and management of the SO and SI which oversee and manage the operations and risk management functions of the system should comprise suitable members with appropriate knowledge, skills and experience to fulfill their roles and responsibilities in relation to the system.

2.3.2. The SO and SI of a designated RPS should have in place a robust and sound risk management framework, commensurate with the nature, scale and complexity of the business of the system, for the identification, measurement, monitoring and management of risks that arise in or are borne by the system. Key risk types typically applicable to designated RPSs include but are not limited to operational risks, technology and cyber-security risks, information risks, financial risks (e.g. business risk, credit risk, settlement risk, liquidity risk), reputational risks, legal and compliance risks, and money laundering and terrorist financing risks. The board and management of the SO and SI which oversee and manage a designated RPS should determine an appropriate level of risk tolerance and capacity for the system, and put in place policies, procedures and controls that are commensurate with the risk tolerance and capacity of the system. In

particular, there should be effective risk management, compliance, and audit functions with sufficient independence and authority. A designated RPS should also have policies in place targeted at ensuring participants and, where relevant, their customers, manage and contain the risks that they may pose to the system. New payment products and services, scheme rules and operational processes, as well as major changes to the existing ones, should be subject to comprehensive risk assessments and all risks identified should be properly addressed before launch. Risk profiles of existing products, services and operational processes should also be reviewed on a regular basis and when there is a change in relevant circumstances, and be updated as appropriate.

2.3.3. The SO and SI of a designated RPS should have in place appropriate control mechanisms to ensure proper functioning of the system. Effective measures should be in place to prevent, detect and handle system disruptions and instances of irregularities, errors and fraud, and to ensure compliance with relevant statutory and regulatory requirements. Independent and risk-focused audit should be conducted regularly to ensure the safety and efficiency of the system.

2.3.4. A designated RPS should have systems and procedures for ensuring that any issue, complaint or enquiry received from the public is handled and addressed in a proper and effective manner.

2.3.5. The governance arrangements, risk management framework and control mechanisms of a designated RPS should be properly documented and subject to periodic review.

2.3.6. The SO and SI of a designated RPS, where appropriate, should have in place adequate resources and controls to ensure that information and documents requests in relation to the system from the HKMA are handled in a responsive manner.

2.3.7. The SO and SI of a designated RPS should implement effective measures to detect and address potential violations of statutory and/or regulatory requirements that may have implications on the safety or efficiency of the

system.

2.4. Financial soundness

2.4.1. The SO and SI of a designated RPS should have in place an appropriate financial risk management framework to ensure that adequate financial resources are available to the system for both its day-to-day operation and development. The financial risk management framework should include (but not be limited to) the following:

(a) *Business risk management* – a robust system to identify, monitor and manage general business risks of the designated RPS, with adequate liquid assets to continue the system's operation and services as a going concern, and if need be, enable orderly winding down of the system;

(b) *Credit risk management* – a robust system to effectively manage the designated RPS's credit exposures to its participants and those arising from its payment, clearing and settlement processes, and maintain adequate financial resources to cover the system's credit exposures; and

(c) *Liquidity risk management* – a robust system to effectively manage the designated RPS's liquidity risks from its participants and other relevant parties, which should, at a minimum, include close monitoring of settlement and funding flows on an ongoing and timely basis and maintain adequate liquid resources in all relevant currencies to ensure smooth settlement of relevant transactions.

2.5. Operational reliability and robustness

Operational reliability

2.5.1. The SO and SI of a designated RPS should implement effective measures to ensure that the infrastructure associated with the system provides adequate and continued services so as to minimize disruptions to retail payment transactions, clearing and settlement processes, and to promote retail payment transaction integrity, confidentiality and availability.

2.5.2. A designated RPS should have clearly defined operational reliability objectives (e.g. operational performance objectives and service-level targets) and policies that are designed to achieve such objectives. The performance of the system against the established objectives should be assessed on a regular basis.

2.5.3. The operational capacity of a designated RPS should be scalable to handle stress volumes, taking into account the operational reliability objectives. The capacity and performance of a designated RPS should be monitored, reviewed and tested on an ongoing basis. The SO and SI of a designated RPS should also conduct demand forecasts and make appropriate plans to handle plausible changes in the volume of business or technical requirements of the system, and conduct system capacity stress testing regularly to validate whether the system can handle large volumes of transfer orders under different extreme but plausible circumstances.

Operational risk management

2.5.4. The SO and SI of a designated RPS should have in place a robust, adequate and effective operational risk system to ensure that payment transactions effected through the system are transferred, cleared and/or settled (as applicable) in a timely, accurate and reliable manner.

2.5.5. The SO and SI of a designated RPS should identify the operational processes and equipment that are of crucial importance for the functioning of the system, and monitor the performance of the system. Arrangements should also be in place to detect anomalies in such processes and equipment, such that emergence of possible incidents can be identified and addressed at an early stage.

2.5.6. The SO and SI of a designated RPS should have in place a comprehensive incident management framework with documented procedures and sufficient management oversight to record, report, analyse, respond to and recover from all operational incidents properly with respect to the system, including, among others, those arising from or involving the system's participants and participants' customers. This should include:

(a) a system for classifying incidents and operational problems according to their criticality and for determining the escalation and handling procedures;

(b) reporting to the HKMA of material incidents which may have implications to the safety or efficiency of the designated RPS as soon as practicable;

(c) an effective strategy for communicating with participants and other stakeholders upon the occurrence of incidents to address their possible concerns and restore their confidence in the system; and

(d) post-incident review to identify the root causes of the incident and any necessary enhancement to the operation and/or business continuity arrangements. The review should, where relevant, include participants of the designated RPS.

2.5.7. A designated RPS should have in place adequate measures to prevent and detect, and mitigate the risks posed by and the impact of, fraudulent transactions carried out through the system, which include monitoring of payment activities carried out through the system and taking prompt actions against fraud and any risks posed by such activities. Proper arrangements should also be put in place to facilitate participants in sharing information and conducting customer education that are relevant to fraud awareness so as to reduce the risk of fraud.

Outsourcing and support service arrangements

2.5.8. Where certain operations of a designated RPS are outsourced to service providers, or support services are provided by service providers, the SO and/or SI concerned should ensure that the outsourcing or support service arrangement will not impair the safety or efficiency of the system. The SO and/or SI remains solely responsible for meeting any statutory and regulatory requirements applicable to the designated RPS.

2.5.9. A proposed outsourcing or support service arrangement should be subject

to comprehensive risk assessment and all risks identified should be properly addressed before implementation of the arrangement. Outsourcing or support service agreements with service providers should be established to clearly set out the outsourcing or support service arrangements, rights and obligations of the parties involved, and measurable performance standards. An effective management programme should be in place to ensure that the outsourced operations or support services continue to meet the required performance standards, any risks arising from the outsourcing or support service arrangements are timely identified and mitigated, and that the outsourcing or support service agreements are regularly reviewed and amended accordingly where appropriate for necessary updates in view of changes in market standards, operational needs and external environment.

Business continuity management (BCM)

2.5.10. The SO and SI of a designated RPS should have in place adequate BCM programmes that are appropriate to the nature, scale, and complexity of the business of the designated RPS, and implement such BCM programmes quickly and effectively in the event of service disruptions, including those caused by service providers. The BCM programmes should identify and address events that may pose a significant risk of disrupting operations of the system, in particular events that could cause a wide-scale and major disruption. The BCM programmes should include proper business impact analyses, recovery objectives and strategies, business continuity plans and alternative sites for business and IT recovery to ensure timely resumption of critical operations following a service disruption. The BCM programmes should be properly documented and subject to regular review and testing.

2.6. Security

2.6.1. The SO and SI of a designated RPS should have a sound and robust security framework that addresses all potential vulnerabilities of and threats to the designated RPS. The security framework should be based on regular analyses of security risks of the system and conform to relevant industry standards. Compliance with the security framework should be monitored

on an ongoing basis.

2.6.2. The security framework of a designated RPS should include, among others:

(a) robust access controls, including physical and logical controls, to prevent unauthorized individuals and applications from accessing or operating the system;

(b) adequate data security measures covering the ownership, classification, inputting, transmission, processing, access, storage and retention of data so as to ensure the confidentiality, integrity, authenticity and privacy of data collected and used by the designated RPS;

(c) adequate payment security measures commensurate with risks arising from different types of transactions processed by the designated RPS, including the authentication and transmission of payment transactions, to prevent unauthorized activities;

(d) comprehensive cyber resilience framework to effectively guard against and recover from cyberattacks, and which should be readily adapted to protect the system against and respond to cyber threats that may arise in the future. The cyber resilience framework, at a minimum, should continuously monitor the trends in cyber threats, implement sufficient protective measures to address different attack scenarios, including attacks which affect the operation of critical IT sites and systems comprising the designated RPS, and perform regular penetration testing and security reviews.

2.7. Settlement certainty

2.7.1. A designated RPS should have clear rules and procedures to provide for certainty as to the circumstances under which transfer orders effected through the system are to be regarded as settled for the purposes of the system. Where settlement may be subject to adjustments (e.g. charge-back arrangements) and/or qualification (e.g. force majeure events), the relevant rules and processes should be clearly set out.

3. EFFICIENCY REQUIREMENTS

3.1. Introduction

3.1.1. Under section 8(2) of the PSSVFO, reference to the efficiency of an RPS includes in particular any matter relating to (a) the speed and efficiency with which operations relating to transfer orders within the system are carried out; (b) the overall cost to a participant of his participation in the system, having regard to the services provided by the system to its participants; and (c) the reasonableness of criteria for admission as a participant in the system.

3.1.2. This Chapter sets out the high-level principles that the MA adopts in assessing whether the operations of a designated RPS are conducted in an efficient manner calculated to minimize the likelihood of disruption to the functioning of the system, taking into account the matters stipulated in section 8(2) of the PSSVFO.

3.1.3. Please also take note of paragraphs 2.3.1, 2.3.3, 2.3.7, 2.5.6 and 2.5.8 in Chapter 2 of the Guideline, which refer to matters related to the efficiency of a designated RPS.

3.2. General

3.2.1. "Efficiency" is a broad concept and generally encompasses the manner in which a designated RPS is operated and the resources required by it in performing its functions and providing its services. A designated RPS should operate efficiently while maintaining appropriate standards of safety. A designated RPS should have in place mechanisms for regular review of its efficiency, taking into account, among others, the speed of transfer, clearing and settlement operations, the operating structure (including any outsourcing and support service arrangements, use of technology and communication procedures), and the overall costs to its participants. The efficiency considerations should always be balanced against the safety of the system.

3.3. Speed and efficiency of operation

3.3.1. The SO and SI of a designated RPS should ensure that:

(a) payment orders are transferred, cleared and/or settled (as applicable) at a reasonable speed, including at peak times or on peak days, having regard to the system's service-level targets, the needs of its participants, the markets it serves and relevant industry standards;

(b) technical arrangements of the system are sufficiently flexible to respond to changing demand and new technologies;

(c) changes in transaction volume or patterns are monitored to plan for necessary system development and/or operational enhancement, with a view to maintaining a reasonable speed for the transfer, clearing and settlement of payment orders; and

(d) where appropriate, adequate liquidity arrangements are in place for efficient settlement of payment obligations.

3.4. Admission criteria

3.4.1. The criteria for admission as a participant in a designated RPS should be objective, transparent, justified having regard to the safety and efficiency of the system and the markets it serves, and commensurate with the system's specific risks. A designated RPS should set reasonable risk-related admission requirements so as to control the risks posed to the system by actual or prospective participants.

3.4.2. A designated RPS should have in place adequate measures to continuously monitor and effectively enforce compliance with the established criteria for admission as a participant in the system, including procedures on the suspension from participation or withdrawal of admission of a participant which breaches or no longer fulfills the admission requirements. A designated RPS should clearly set out criteria under which access to the system by its participants may be suspended or withdrawn, and the

procedures for facilitating the suspension or orderly exit of a participant.

4. REQUIREMENTS ON OPERATING RULES

4.1. Introduction

4.1.1. Operating rules are defined in section 2 of the PSSVFO as the rules or terms that govern the operation, use or functioning of an RPS. Section 7(1)(b) of the PSSVFO requires the SO and SI of a designated RPS to ensure that there are in place in relation to the system operating rules that (i) comply with the requirements specified in section 7(2) of the PSSVFO and with any prescribed requirements relating to the operating rules of a designated RPS, and (ii) provide for the system to be operated in accordance with the PSSVFO as it applies in relation to that system. Section 7(1)(c) of the PSSVFO further requires that the SO and SI of a designated RPS shall ensure that adequate arrangements are in place to monitor and enforce compliance with the operating rules of the system, including arrangements regarding the resources available to the SO.

4.1.2. This Chapter sets out the high-level principles that the MA adopts in assessing compliance with the abovementioned requirements.

4.2. Design of operating rules

4.2.1. The operating rules of a designated RPS should be clear, unambiguous, enforceable, up-to-date and consistent with the applicable laws and regulations, and available to all participants. The operating rules of a designated RPS should cover, among other things:

(a) mechanisms to deal with insolvency and default of participants that are appropriate and adequate for the system in all circumstances, including that a participant may be suspended when it becomes insolvent. A participant should be required to notify the SO and SI concerned as soon as practicable when it becomes, or is likely to become, unable to meet its obligations. In case the problem has a significant implication on the functioning of the system, the SO and SI should inform the HKMA and the relevant stakeholders in a timely

manner;

(b) arrangements to deal with situations where the SO or SI of the system is likely to become unable to meet its obligations under the system; and

(c) rules and terms providing for the system to be operated in accordance with the PSSVFO, having regard to the safety and efficiency requirements outlined in Chapters 2 and 3 above and other relevant guidance issued by the MA.

4.2.2. It is the responsibility of the SO and SI of a designated RPS to ensure that the operating rules of the system and any procedures or manuals established under the operating rules (including any changes to the foregoing) are in compliance with the PSSVFO and other applicable statutory and/or regulatory requirements, having regard to any relevant guidance issued by the MA. The SO and SI of a designated RPS shall take appropriate actions, including seeking the MA's approval for changes to the operating rules, to bring the operations of the system in compliance with applicable statutory and/or regulatory requirements, having regard to any relevant guidance issued by the MA. Note that under section 7(3) of the PSSVFO, the MA's prior written approval is required for any changes to the operating rules of a designated RPS.

4.2.3. The MA may issue additional guidelines or requirements under the PSSVFO in connection with the performance of the MA's functions under PSSVFO, which include (among others) promoting and encouraging proper standards of operation and sound and prudent practices among designated RPSs. The SO and SI of a designated RPS shall take appropriate actions, including changing the operating rules, procedures or manuals of the system, to bring the system's operations in line with the relevant guidelines and requirements issued by the MA.

4.3. Arrangements to monitor and enforce compliance with the operating rules

4.3.1. The SO and SI of a designated RPS should put in place effective control mechanisms to ensure that the system is operated in accordance with the established operating rules and to monitor participants' compliance with relevant rules on an ongoing basis.

4.3.2. Where detailed procedures and manuals are established under the operating rules for particular areas of the operation of the system, effective control mechanisms should be in place to ensure that the underlying procedures and manuals are consistent with the operating rules at all times.

4.3.3. The SO and SI of a designated RPS should have in place processes for promptly and duly informing participants and relevant stakeholders (as appropriate) of any changes to the operating rules of the system.