HONG KONG MONETARY AUTHORITY
香港金融管理局

ADDITIONAL GUIDANCE ON OVERSIGHT OF DESIGNATED RETAIL PAYMENT SYSTEMS

September 2022

Structure

Introduction

1.1. The Guideline on Oversight of Designated Retail Payment Systems (Guideline) issued by the Hong Kong Monetary Authority (HKMA) sets out the high level principles that the HKMA adopts in overseeing designated retail payment systems (RPSs). To assist system operators (SOs) and settlement institutions (SIs) of designated RPSs in better understanding the standards by which the principles set out in the Guideline should be applied, the HKMA issues this additional guidance to provide further guidance in respect of specific sections or paragraphs of the Guideline as and when necessary.

1.2. SOs and SIs of designated RPSs should regard this additional guidance as illustrations of how a specific principle requirement can be met in typical situations. They are expected to see through the illustrations and strive to achieve compliance with the Guideline by appropriately customizing their systems of controls, taking into account their specific situations. This additional guidance should be read in conjunction with the relevant sections in the Guideline.

1.3. For the avoidance of doubt, this additional guidance is applicable to credit card transactions as well as debit card transactions that are subject to similar arrangements (e.g. involvement of third-party service agents). In addition, the regulatory requirements on designated RPSs are set out in the Payment Systems and Stored Value Facilities Ordinance and the Guideline. While this additional guidance seeks to help SOs and SIs of designated RPSs better understand how they may comply with those requirements, the additional guidance does not have any effect of overriding or replacing any provisions in those documents.

1.4. For the sake of conciseness, this additional guidance only includes sections or paragraphs of the Guideline on which additional guidance are provided. Going forward, the HKMA may revise the additional guidance or issue further guidance on other sections or paragraphs of the Guideline in the form of amendments to this additional guidance as and when necessary.

Relevant requirements from Guideline on Oversight of Designated Retail Payment Systems ("Guideline") (issued in September 2020)

2. Safety Requirements

Guideline section 2.2 – Legal basis

Guideline 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.*

Guideline section 2.3 – Governance, risk management and control procedures

Guideline 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.*
Guideline 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.*

4. Requirements on Operating Rules

Guideline section 4.3 – Arrangements to monitor and enforce compliance with the operating rules

Guideline 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.*

Additional guidance

Additional guidance (a)	The SO and SI of a designated RPS should have in place a robust framework that can require its participants to rectify data breaches that occur at their third-party service agents.
Additional guidance (b)	The SO and SI of a designated RPS should require its participants (e.g. card issuers and merchant acquirers) to: (i) conduct due diligence and validate compliance with applicable due diligence standards prior to engaging third-party service agents (e.g. paying agents and payment gateways); and (ii) have contracts/service agreements with their third-party service agents that set out clearly the rights and obligations of the parties involved.
Additional guidance (c)	The contracts/service agreements between participants and their third-party service agents should be enforceable, enabling the participants, or the SO and SI of the relevant designated RPSs where appropriate to take necessary actions against a participant's third-party service agents for rectification of data breaches that occur at such third-party service agents.
Additional guidance (d)	The contracts/service agreements should also require the third-party service agents engaged by the participants to comply with the standards/requirements (e.g. generally accepted industry data security standards) as promulgated by the SO and SI of the designated RPSs. Such standards/requirements should include, among others, data security standards to effectively prevent, detect, mitigate and timely report data leakages and cyberattacks. In particular, incidents that the SO and SI reasonably consider may have material and adverse impacts on the cardholders in Hong Kong or on the safety and efficiency of the designated RPS' payment card operations in Hong Kong should be reported in a timely manner.

2. Safety Requirements

Guideline section 2.5 – Operational reliability and robustness

Guideline 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.*
Guideline 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.*
Guideline 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.*

Guideline section 2.6 – Security

Guideline 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.*
Guideline 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.*

Additional guidance

(I) ***Prevention***

Additional guidance (a)	The SO and SI of a designated RPS should have in place appropriate standards/requirements, such as generally accepted industry data security standards that the SO and SI consider to be applicable to the operations of the designated RPS, that provide a baseline of technical and operational requirements designed to protect payment data and payment card credentials. Such standards/requirements should be applicable to the designated RPS and via applicable arrangements (e.g. rules and procedures of the scheme, contractual arrangements between participants and their third-party service agents), be cascaded down to all entities (e.g. its participants and where applicable, the customers and third-party service agents of its participants) that store, process, or transmit card data and/or sensitive authentication data, or could impact the security of the card data environment. Such standards/requirements should include, at a minimum, classification of sensitive data, strong encryption of payment data, robust key management, proper logical and physical access controls, data retention and disposal, effective anti-malware and anti-phishing mechanisms.
Additional guidance (b)	The SO and SI of a designated RPS should have in place appropriate arrangements such as scheme rules and procedures so that only entities (e.g. its participants and where applicable, the customers and third-party service agents of its participants) that can satisfactorily demonstrate on a regular basis their compliance with the relevant security standards/requirements should be allowed to store, process, or transmit card data and/or sensitive authentication data in relation to that designated RPS. To that end, the SO and SI of a designated RPS should put in place arrangements to, with assistance from its participants where necessary, regularly identify entities that should comply with such standards/requirements.
Additional guidance (c)	The SO and SI of a designated RPS should take steps to develop or promulgate appropriate protocols or arrangements that help prevent unauthorized transactions, having regard to relevant factors such as technological evolution, such that even if card credentials are leaked, a fraudster could not easily use them to conduct fraudulent transactions. In the scenario of online transactions, examples of such protocols or arrangements are tokenisation of card credentials and authentication of card transactions using 3-D Secure.

(II) ***Detection***

Additional guidance (a)	The SO and SI of a designated RPS should put in place requirements, such as having rules and procedures, on its participants to: (i) periodically monitor their third-party service agents' compliance with data security standards as promulgated by the SO and SI of such designated RPS; and (ii) timely report suspected and/or actual data breaches and cyberattacks that take place at their third-party service agents to the SO and SI of the designated RPS. In particular, incidents that the SO and SI reasonably consider may have material and adverse impacts on the cardholders in Hong Kong or on the safety and efficiency of the designated RPS' payment card operations in Hong Kong should be reported in a timely manner.
Additional guidance (b)	There should be appropriate and risk-based approaches to validate the relevant entities' compliance with the corresponding security standards/requirements, which are promulgated by the SO and SI of such designated RPS and cascaded down to relevant entities via applicable arrangements such as scheme rules and procedures, as well as contractual arrangements between participants and their third-party service agents. Examples of such validations are regular and documented validations and validations upon significant change to the environments relevant to those standards/requirements. The SO and SI of a designated RPS should also have in place appropriate and risk-based measures to, via the cascade-down arrangements, require the relevant entities to demonstrate their compliance with the relevant security standards/requirements and promptly handle any non-compliance.
Additional guidance (c)	The SO and SI of a designated RPS should have in place fraud monitoring systems to detect anomalies in card transaction patterns and analyse fraud information reported by its participants, which may in turn help identify suspicious and/or actual data breaches at an early stage.

(III) ***Mitigation***

Additional guidance (a)	Once the SO and SI of a designated RPS are aware of suspected and/or actual data leakages and cyberattacks incidents, they should take appropriate actions, including responding swiftly and if needed, requiring its participants and/or, via the cascade-down arrangements, requiring its participants' third-party service agents, to initiate and provide necessary assistance to forensic investigations, to: (i) identify the cause of failure; (ii) address the data security issues; and (iii) implement mitigating measures, with a view to preventing similar incidents from happening.
Additional guidance (b)	The SO and SI of a designated RPS should take appropriate and risk-based enforcement actions against non-compliance with data security standards by its participants, and should, via the cascade-down arrangements, require its participants to take appropriate actions against non-compliance with data security standards by their third-party service agents. Examples of such actions may range from enhanced review or validations, enhanced data security measures/requirements, warnings, fines, to prohibition from accessing the designated RPSs' networks.
Additional guidance (c)	The SO and SI of a designated RPS should have in place mechanisms to share data breaches and fraud information and/or intelligence with its participants in a timely, effective and appropriate manner so as to help increase the fraud awareness of its participants and facilitate its participants to take appropriate actions, such as strengthened fraud monitoring, timely customer notification, and consideration of change of payment cards.

(IV) ***Incident reporting***

Additional guidance (a)	The SO and SI of a designated RPS should put in place arrangements to ensure timely notification and efficient flow of information on data breach incidents of other parties involved in a transaction cycle (e.g. merchant acquirers and payment gateways) associated with their networks, in addition to incidents of their own systems to the HKMA. In particular, incidents that the SO and SI reasonably consider may have material and adverse impacts on the cardholders in Hong Kong or on the safety and efficiency of the designated RPS' payment card operations in Hong Kong should be reported in a timely manner.

Additional guidance (b)	In assessing whether an incident is material and/or warrants reporting to the HKMA, the SO and SI of a designated RPS should have regard to relevant factors including but not limited to the following: (i) Incidents having significant adverse impact on the functioning, reliability, safety and efficiency, robustness, integrity of information, risk management and control, soundness and/or stability of the designated RPS in Hong Kong (e.g. cyberattacks affecting system operation, data leakages); (ii) Incidents relating to transactions processed within the designated RPS that have caused or may cause material financial impact on or financial loss to a substantial number of parties in Hong Kong, such as its operator, participants and, where relevant, customers of participants, regardless of whether there are arrangements for handling any financial impact/losses of such incidents (e.g. chargeback); (iii) Suspected or actual fraud or data breaches of a significant scale that have material or adverse impacts on the cardholders in Hong Kong; and (iv) Incidents which may lead to material and adverse reputational risk to, or affect the confidence of the general public in Hong Kong in, the designated RPS.
Additional guidance (c)	Once the SO and SI of a designated RPS become aware of an incident having material and adverse impacts on the cardholders in Hong Kong or on the safety and efficiency of its payment card operations in Hong Kong, such as cyberattack which affects system operation or data leakage, the SO and SI should notify the HKMA promptly and provide the HKMA with any available information related to such incident at the time (e.g. root cause, expected or actual impact, remedial actions taken or to be taken, and responses to potential enquiries).
Additional guidance (d)	The SO and SI of a designated RPS should assess whether an incident involves potential or actual breach that should be reported to other regulator(s) pursuant to its obligations under any applicable law or regulation other than those relevant to the designated RPS regime (e.g. pursuant to the Personal Data (Privacy) Ordinance). If so, the SO and SI of the designated RPS should report such an incident to the relevant regulator(s) in addition to the HKMA.
Additional guidance (e)	For the avoidance of doubt, the SO and SI of a designated RPS should not wait until all relevant information is gathered and/or the problem is rectified before reporting to the HKMA any incident that the SO and SI reasonably consider may have material and adverse impacts on the cardholders in Hong Kong or on the safety and efficiency of its payment card operations in Hong Kong. In cases where further investigations are required to ascertain basic facts related to the incident, early alert should also be provided to the HKMA instead of after the investigations.

Additional guidance (f)	The HKMA may request the SO and SI of a designated RPS to provide further information or updates (e.g. preliminary and final investigation findings, where applicable).