

CODE OF PRACTICE FOR PAYMENT CARD SCHEME OPERATORS

Background

The Code of Practice for Payment Card Scheme Operators (“the Code”) has been drawn up and observed by eight payment card scheme operators¹ (“scheme operators”) in Hong Kong since 2007. The introduction of the Payment Systems and Stored Value Facilities Ordinance (“the Ordinance”) on 13 November 2015 has necessitated certain modifications of the Code, which are now incorporated in this version. The scheme operators remain committed to observe this updated version of the Code in providing services to the general public.

Purpose

This Code specifies general principles for the scheme operators to observe in order to promote the general safety and efficiency of payment cards in Hong Kong and to foster public confidence in them.

Classification

This is a non-statutory Code drawn up by the scheme operators in Hong Kong. New scheme operators entering the Hong Kong market should also adhere to the general principles in this Code.

Application

To the scheme operators in Hong Kong. This Code applies only to their operations in Hong Kong and is not intended to have extra-territorial effect.

¹ “Payment card scheme operators” means, for the purposes of this Code, multi-purpose payment card schemes which provide credit and /or debit function through a payment network for making payment of goods or services. It excludes multi-purpose stored-value cards, which are dealt with separately by the regulatory regime for stored value facilities under the Ordinance.

Structure

INTRODUCTION

1. Status of the Code
2. Objectives
3. Enquiries

SAFETY

4. Legal Basis of the System
5. Rules and Procedures
6. Operational Reliability and Business Continuity
7. Security
8. Governance Arrangements
9. Data Security and Integrity
10. Financial Requirement

OPERATIONAL EFFICIENCY

11. Operational Efficiency

TRANSPARENCY

12. Participation Criteria
13. Transparency and Competition

MONITORING REQUIREMENTS

14. Prudential Supervision
15. Data Collection
16. Incident Reporting
17. Compliance

INTRODUCTION

1. Status of the Code

- 1.1. This Code has been drawn up by the eight scheme operators that have payment card operations in Hong Kong currently. They are American Express International, Inc., UnionPay International Co., Ltd., Discover Financial Services (Hong Kong) Limited, JCB International (Asia) Ltd., MasterCard Asia/Pacific Pte. Ltd., Visa Worldwide Pte. Limited, EPS Company (Hong Kong) Limited and Joint Electronic Teller Services Ltd. (JETCO). The development of the Code was overseen and has been endorsed by the Hong Kong Monetary Authority (HKMA).

A payment card scheme generally involves either of the following:

- (a) three operational parties, namely the scheme operator, which is both a card issuer and merchant acquirer (although sometimes third parties are contracted or franchised to perform these activities), merchants and cardholders – these schemes are referred to as “three-party schemes”; or
 - (b) where the scheme is operated on a platform provided by the scheme operator, four operational parties, namely card issuers, merchant acquirers (although sometimes scheme operators may act as the merchant acquirers), merchants and cardholders – these schemes are referred to as “four-party schemes”.
- 1.2. This Code is not legally binding and does not confer legal rights on, or give rise to legal rights or liabilities against, any scheme operator, the HKMA or any other person or legal entity. Nevertheless, with the objective of promoting the general safety and efficiency of payment cards operations in Hong Kong and to foster public confidence in such operations, by signing this Code each scheme operator declares its intention to make reasonable efforts to comply with it. Each scheme operator will monitor such compliance and will report on its compliance status to the HKMA. The HKMA will monitor the overall implementation of the self-compliance with this Code and will work with the scheme operators to follow-up on non-compliance issues, if any.
- 1.3. Where applicable, the principles in this Code apply to the daily operations of scheme operators in Hong Kong, notwithstanding that each scheme operator has its own mode of operation. The principles in this Code also apply to each scheme operator’s overall relationship with, in the case of an operator of a three-party scheme, its cardholders and merchants in Hong Kong and, in the case of an operator of a four-party schemes, its card issuers and merchant acquirers in Hong

Kong.

- 1.4. The provisions of this Code are supplementary to and do not supplant any relevant legislation, codes, guidelines or rules applicable to institutions authorized under the Banking Ordinance or to systems designated under the Ordinance.
- 1.5. The Code is subject to review and revision from time to time by the scheme operators with the endorsement of the HKMA.

2. Objectives

- 2.1. This Code is intended to promote the general safety and efficiency of payment card operations in Hong Kong and to foster public confidence in payment card operations.

3. Enquiries

- 3.1. Due to the differences in the ownership or membership structure, phases of development, business model and operation mode of each payment card scheme, each scheme operator's interpretation of this Code is applicable only to itself and does not necessarily represent or reflect the interpretation of any one or more or all of the other scheme operators.
- 3.2. Enquiries about this Code should be addressed to the relevant scheme operators. Their contact information can be obtained from their Hong Kong corporate or their head offices websites.
- 3.3. This Code can be viewed or downloaded from the website of each of the scheme operators, if any, and of the HKMA.

SAFETY

4. Legal Basis of the Operation

- 4.1. Each scheme operator should have a sound legal basis for its payment card operations in Hong Kong, together with appropriate rules and procedures.
- 4.2. Appropriate processes should be in place to ensure that rules and procedures as well as the contractual relationships with its relevant parties (e.g. merchant acquirers and card issuers, merchants and cardholders, where applicable) should be valid and enforceable. Where applicable, this should include clear rules and procedures to regulate authorization, clearing and settlement for both domestic and cross-border transactions.

5. Rules and Procedures

- 5.1. Each scheme operator of a four-party scheme should have rules and procedures of the scheme that enable its merchant acquirers and card issuers to obtain sufficient information regarding their respective rights and obligations associated with their participation in its payment card scheme. Such rights and obligations must be clearly defined and disclosed to its merchant acquirers and card issuers. Rules and procedures of the scheme should be complete, up-to-date and readily available to all its merchant acquirers and card issuers; and they should be duly informed of any relevant changes in the rules and procedures.
- 5.2. Each scheme operator of a three-party scheme should have, and each scheme operator of a four-party scheme should encourage its card issuers and/or its merchant acquirers (as applicable) to have, rules and procedures covering the following areas:
 - (a) the liabilities of cardholders for any loss arising from unauthorized use of the card; and
 - (b) the arrangements to handle charge-backs, if applicable, and disputes over cardholders' liability with respect to unauthorized transactions.
- 5.3. Each scheme operator of a three-party scheme should have, and each scheme operator of a four-party scheme should have and encourage its merchant acquirers and card issuers to have, clear procedures for the processes of setting fees and charges.

6. Operational Reliability and Business Continuity

- 6.1. Each scheme operator should have sound and prudent management, administrative, accounting and control procedures managing the financial and non-financial risks to which it reasonably considers it may be exposed.
- 6.2. Each scheme operator should conduct risk analysis on new payment card products. In addition, where it reasonably believes that there has been a change of relevant circumstances, each scheme operator should perform a review on the risk profile of existing products to assess risks relating to product security and continuity.
- 6.3. Each scheme operator should seek to ensure that it has an adequate number of properly trained and competent personnel to operate its system at a level it considers appropriate in all situations that it considers are reasonably foreseeable.

- 6.4. Each scheme operator of a four-party scheme should provide its merchant acquirers and card issuers with information it reasonably considers relevant to fraud awareness in the context of the operation of its payment card scheme. Each scheme operator of a three-party scheme should provide, and each scheme operator of a four-party scheme should encourage its card issuers and merchant acquirers to provide, its/their cardholders and merchants with education it reasonably considers relevant to fraud awareness and the proper use or processing of cards to reduce the risk of fraud.
- 6.5. Each scheme operator should have comprehensive, rigorous and well-documented operational and technical procedures to address reasonable operational reliability, the integrity of its network and the timeliness of transactions in the face of malfunctions, system interruption and transmission failures or delays. Each scheme operator should also have in place a reasonable, effective, well-documented and regularly-tested business contingency plan addressing system functionality in the event of unforeseen interruption.
- 6.6. Each scheme operator should have a thorough due diligence and management oversight process for managing its outsourcing relationships, if any, that it considers may impact the operation of its payment card system. The liabilities and responsibilities between the scheme operator and its outsourcing service providers should be clearly defined.
- 6.7. Each scheme operator should design its technical system for payment card processing with sufficient capacity to enable its ongoing operations, which should be monitored periodically and upgraded when the scheme operator considers reasonably necessary.
- 6.8. Each scheme operator should have sufficient clearing and settlement arrangements to enable efficient, reliable and secure operation of its payment card system.
- 6.9. Each scheme operator should review periodically its security objectives, policies and operational services.
- 6.10. Each scheme operator of a three-party scheme should have, and each scheme operator of a four-party scheme should encourage its merchant acquirers and card issuers to have, well-defined procedures to respond to payment card security-related incidents. The procedures should encompass a consistent and systematic approach in handling an incident.
- 6.11. As a follow-up to each security-related incident materially affecting the scheme operator, its merchant acquirers, card issuers, and/or merchants that accept its payment cards, each affected scheme operator should

initiate a confidential post-incident assessment of the situation by the parties it considers appropriate having regard to the nature of the incident to seek to identify the root cause of the incident, weakness leading to the incident and other potentially vulnerable areas underlying the incident.

7. Security

7.1. Each scheme operator of a three-party scheme should adopt, and each scheme operator of a four-party scheme should encourage its merchant acquirers and card issuers to adopt, appropriate and commercially reasonable technical security measures and procedural safeguards to protect the security of its system. Each scheme operator should also consider adopting international technical security standards where appropriate. Such measures might include:

- (a) requirements to build and maintain a secure network, including conditions to install and maintain firewalls to protect data, and a change of vendor-supplied default system passwords and other security passwords;
- (b) requirements to help protect data through the entire life cycle of a transaction; particularly on control measures to access data, procedures for storing cardholder and transaction data, and disposal of cardholder and transaction information after use;
- (c) conditions to use and regularly update anti-virus software, and to develop and maintain secure systems and applications; and
- (d) requirements to manage cyber security risk effectively, including the capability to keep pace with the trends of cyber attacks.

7.2. In addition, each scheme operator should have mechanisms which allow it to monitor on an ongoing basis attempted security breaches that may compromise its systems. There should be measures to control access and to regularly monitor and test card operation networks. To the extent possible, there should be a policy that addresses information security for all related parties, such as employees and contractors.

7.3. Each scheme operator should conduct periodic security reviews of its system. Such reviews could be performed either by the scheme operator or, at its discretion, by an independent party appointed by it.

8. Governance Arrangements

8.1. Each scheme operator should have clearly defined and documented organizational arrangements, such as ownership and management structure. Each should operate as it deems fit, with appropriate

segregation of duties and internal control arrangements so as to reduce the likelihood of mismanagement and fraud.

- 8.2. Each scheme operator should have reasonably effective measures and controls to ensure compliance with the Code.

9. Data Security and Integrity

- 9.1. Each scheme operator should be responsible for the security and integrity of all payment card data and records maintained or controlled by it, such as transaction information. Each scheme operator of a three-party scheme should have, and each scheme operator of a four-party scheme should encourage its merchant acquirers and card issuers to have, rules and procedures to safeguard the necessary confidentiality of all data and records in its control, including cardholder and transaction information. Each scheme operator of a three-party scheme should uphold, and each scheme operator of a four-party scheme should encourage its merchant acquirers and card issuers to uphold, generally accepted industry data security standards that it considers to be applicable to its operations.
- 9.2. Each scheme operator should establish and maintain, where possible, procedures it considers to be reasonable for the recovery of transaction data that is necessary for its daily operation in the event of system failure.

10. Financial Requirement

- 10.1. The financial condition of each scheme operator should be sound and viable.

OPERATIONAL EFFICIENCY

11. Operational Efficiency

- 11.1. Each scheme operator should aim to provide a reasonably convenient and practical means of making payments to its cardholders in Hong Kong.
- 11.2. Each scheme operator should ensure that its system can process transactions at a speed which is reasonably efficient.
- 11.3. Each scheme operator of a three-party scheme should enter into, and each scheme operator of a four-party scheme should encourage its merchant acquirers to enter into, agreements with its/their merchants to specify that the relevant payment card acceptance logo should be

displayed in a visible manner to cardholders (except where the merchant is excused by relevant rules and procedures from doing so).

TRANSPARENCY

12. Participation Criteria

- 12.1. Each scheme operator should have an established process for considering applications to become its merchant acquirer or card issuer, if applicable.
- 12.2. Each scheme operator, if applicable, should have procedures in place to allow prospective merchant acquirers and card issuers to access or obtain the information necessary to determine whether to apply to become a merchant acquirer or card issuer.
- 12.3. The general eligibility and participation criteria should be disclosed to genuine applicants upon request.

13. Transparency and Competition

- 13.1. Each scheme operator should comply with competition laws and guidelines applicable to their payment card business in Hong Kong.
- 13.2. The relevant fees and charges should be documented and communicated clearly to the card issuers, merchant acquirers, merchants and/or cardholders, where applicable.
- 13.3. Each scheme operator is encouraged to inform affected parties of changes to its payment card system that materially affect such parties' financial risk, operational risk, data security risk and legal risk in Hong Kong.

MONITORING REQUIREMENTS

14. Prudential Supervision

- 14.1. Merchant acquirers and card issuers of the scheme operators that are authorized institutions in Hong Kong are subject to the licensing requirements under the Banking Ordinance and hence the prudential supervision by the HKMA.

15. Data Collection

- 15.1. Each scheme operator should submit to the HKMA, to the extent practicable and permitted by law, at such reasonable intervals and in such reasonable manner as specified by the HKMA, readily available

statistics or information which might include, the number of payment cards issued and in circulation, the total volume and value of transactions, the number of terminal facilities, system performance and relevant financial information. Such information submitted shall not be made public in any form without the express written consent of the relevant scheme operator. Each scheme operator may also be reasonably required to provide certain information to the HKMA on an ad hoc basis to enable it to evaluate compliance with this Code. Such information, if the HKMA considers it useful for payment system research, may be published by the HKMA in an aggregate form, provided that to the extent permitted by law, the confidentiality of the data of individual scheme operators is protected at all times.

- 15.2. Each scheme operator should, to the extent permitted by law, inform the HKMA on a confidential basis of major decisions that it is aware of and reasonably considers may materially and adversely affect the general safety and efficiency of its payment card operations in Hong Kong.

16. Incident Reporting

- 16.1. Each scheme operator should ensure a timely and efficient flow of relevant information to the HKMA of any incident (such as data security breaches) that it reasonably considers may have a material and adverse impact on its cardholders in Hong Kong or on the safety and efficiency of its payment card operations in Hong Kong.

17. Compliance

- 17.1. Each scheme operator is expected to perform an annual self-assessment of its compliance with this Code. Its internal auditors, internal compliance officer or appointed independent assessor should perform this self-assessment as part of their on-going duties and provide the HKMA with a copy of their compliance report. Self-assessment reports submitted by each scheme operator are confidential and proprietary to that scheme operator, and shall not be disclosed to any third party.