CODE OF PRACTICE FOR MULTI-PURPOSE STORED VALUE CARD OPERATION

INTRODUCTION

1) Status of the Code of Practice for Multi-purpose Stored Value Card Operation

1.1 This Code of Practice for Multi-purpose Stored Value Card Operation (Code) is issued by Octopus Cards Limited (OCL) and endorsed by the Hong Kong Monetary Authority (HKMA).

1.2 This is a non-statutory Code issued on a voluntary basis. The principles of the Code apply to the daily operation of multi-purpose stored value card, as well as the overall relationship between participants of the operation, including card issuers, system operators, cardholders, merchant acquirers and merchants[1]. The HKMA will monitor the compliance with the Code.

1.3 The recommendations set out in the Code are supplementary to and do not supplant any relevant legislation, codes, guidelines or rules applicable to institutions authorized under the Banking Ordinance or systems designated under the Clearing and Settlement Systems Ordinance.

1.4 The Code is subject to review and revision from time to time.

2) Objectives

2.1 The Code is intended to promote safety and efficiency of multi-purpose stored value card operation by setting out the guiding principles for multi-purpose stored value card issuers, system operators and merchant acquirers to follow in their daily operations; and through this, to foster general public's confidence in the multi-purpose stored value card operation.

3) Enquiries

3.1 Enquiries about the Code should be addressed to OCL. The current address and telephone number of OCL are as follows –

Octopus Cards Limited
46/F, Manhattan Place
23 Wang Tai Road
Kowloon Bay, Kowloon
Hong Kong
Tel: 2266 2200
Fax: 2266 2211
Website: http://www.octopus.com.hk

3.2 The Code can be viewed or downloaded from the websites of OCL and HKMA.

---

[1] "Merchants" in this Code include service providers and load agents.

SAFETY

4) Legal Basis of the System

4.1 There should be sound legal basis for the operation of a multi-purpose stored value card system. Rules and procedures governing the contractual relationships between participants of the system, including the merchant acquirers, merchants, card issuers, system operators and cardholders should be valid and enforceable. For cross-border transactions, rights and obligations stated in the rules must be enforceable under the laws of all relevant jurisdictions.

5) Rules and Procedures

5.1 There should be rules and procedures that enable participants to have a clear understanding of each of the financial and non-financial risks they might incur through participation in the system. Rights and obligations on the part of the respective participants must be clearly defined and disclosed to the relevant participant. Participants should be duly informed of any changes in the relevant rules and procedures. For example, there should be rules stating:

a) the conditions of redemption, such as the obligation of the card issuers to redeem the residual values stored in the card against cash at par value at the request of the cardholder;

b) the time when the payment made by cardholders is irrevocable and irreversible;

c) the liabilities of cardholders for any loss arising from misuse, loss, malfunction, theft of, or damage to the multi-purpose stored value card device;

d) the arrangements to handle disputes over the amount of stored value and cardholders' liability with respect to unauthorized transactions; and

e) the control measures to mitigate possible credit risks assumed by the merchants and the system operators respectively.

6) Security, Operational Reliability and Business Continuity

6.1 Reasonable effort should be made by the system operators to ensure a high degree of security and operational reliability of the system. Robust and well-tested contingency arrangements should be in place to ensure timely completion of daily processing.

7) General

7.1 System operators should have sound and prudent management, administrative, accounting and control procedures managing the financial and non-financial risks to which it may be exposed.

7.2 System operators should ensure that there are adequate numbers of well-trained, competent and trustworthy personnel to operate the system in both normal and abnormal situations. In particular, system operators should provide merchants with training on the operation of payment and value loading devices (if applicable) and fraud awareness.

7.3   Merchant agreements should specify clearly the responsibility of merchants for maintaining security and operational reliability of the system.

8)   Security

8.1   System operators should adopt appropriate and commercially reasonable technical security measures and procedural safeguards to detect and protect the system against fraud and avoid counterfeit. System operators should also consider adopting international technical security standards where appropriate. In addition, there should be mechanisms established to monitor on an ongoing basis attempted security breaches.

8.2   The card issuers and merchant acquirers should adopt appropriate measures to limit cardholders' potential loss arising from the loss of their cards.

8.3   Periodic security audit should be carried out by an independent party on the performance and tamper resistance of the cards, payment and value loading devices, centralized monitoring system and fraud detection mechanism.

9)   Operational Reliability

9.1   There should be comprehensive, rigorous and well-documented operational and technical procedures to ensure operational reliability, which encompasses the robustness of devices and networks and timeliness of transactions in the face of malfunctions, system interruption and transmission failures or delays.

9.2   The system should be designed with sufficient capacity, which should be monitored and upgraded in advance of business changes.

9.3   There should be robust clearing and settlement arrangements to ensure efficient, reliable and secure operation of the system.

9.4   System operators should review periodically its security objectives, policies and operational services.

9.5   System operators should establish a comprehensive due diligence and management oversight process for managing its outsourcing relationships, if any. Operational reliability, information integrity, security procedures and business continuity arrangements should extend to the affected areas, processes and personnel.

10)   Business Continuity

10.1   System operators should have in place an effective, well-documented and regularly-tested business contingency plan to ensure that the system can continue to function in the event of unforeseen interruption.

11)   Governance Arrangements

11.1   System operators should have clearly defined and properly documented organizational arrangements. There should be appropriate segregation of duties so as to reduce the likelihood of mismanagement and fraud. Relevant information on the system and its operations should be complete, up-to-date and readily available to the public.

11.2 System operators must not undertake business activities that are not closely related to multi-purpose stored value card operation.

11.3 System operators should make reasonable effort to establish and maintain effective systems and controls for compliance with the Code.

12) Data Integrity and Retrieval

12.1 System operators should be responsible for the security, integrity and accuracy of all data and records pertaining to the issue and operation of the card scheme, and the related systems.

12.2 System operators should establish clear audit trail of all transactions as well as adequate provision for recovery in the event of loss.

12.3 System operators should ensure that relevant cardholders' transaction information that relates to a specified period, to the extent that such information is appropriately recorded by the system, could be provided to respective cardholders in a readily comprehensible form.

12.4 System operators, card issuers and merchant acquirers should ensure the appropriate degree of confidentiality of all cardholder and transaction information.

13) Financial Requirement

13.1 Card issuers should manage the float on prepayments from cardholders prudently. Such liabilities should be backed at all times by sufficient, liquid, and low risk assets.

13.2 System operators should ensure that they have sufficient cash flow to handle daily operations.

14) Prudential Supervision

14.1 Card issuers of multi-purpose stored value cards are subject to the licensing requirements under the Banking Ordinance and hence the prudential supervision by the HKMA.

EFFICIENCY

15) Operational Efficiency

15.1 System operators should seek to economise on total processing costs (i.e. the costs of handling a transaction, and preparing and executing the resulting settlement entries) with regard to such factors as the needs of its participants, security requirements of the system operators and the current and prospective costs of inputs like labour and technology. Cost and benefit analysis should be conducted before launching new services.

15.2 System operators should ensure that the system can provide merchants with an efficient and productive means for processing transactions. In particular, the system should process transactions at a speed which is reasonably

acceptable to the cardholders and merchants.

15.3 System operators should ensure that the system can provide a convenient means of payment to cardholders, including making a payment and reloading value. System operators should consider using standards which are commonly adopted by other system operators to ensure interoperability provided that the system security is not unduly compromised.

15.4 The system design should be reasonably flexible and responsive to changing demands of cardholders and merchants as well as the technological developments. The system should deliver, at all times, cost effective payment services that satisfy the reasonable needs of cardholders and merchants.

15.5 System operators should not discriminate against cardholders with a disability and should uphold a helpful approach by making available to them services on the same terms and conditions as for other cardholders.

15.6 Merchant agreements should specify that merchants should display the stored value card acceptance logo in a fully visible manner.

16) Participation Criteria

16.1 The system should have objective and publicly disclosed criteria for participation, which permit fair and reasonable access. Imposing restrictions on access by merchants is warranted for protecting the safety and integrity of the system plus other participants from undue risk resulting from the participation of other parties. Where appropriate given the design of the system and when technically feasible, the system operators should aim to share their technical platform with other parties interested in card issuing and merchant acquiring businesses, subject to the required security standards of the system operators and on commercial terms to be agreed between the system operators and the relevant interested parties.

17) Market Access, Fees and Charges

17.1 There should be no measures having the effect of unfairly limiting, or exploiting the absence of, competition in the market. There should be no exclusive trading clause, which prohibits the merchants from using other forms of stored value payment system.

17.2 Fees or charges should have reasonable relation to the cost and investments of providing the relevant service or product, business plans, risk levels and other relevant factors including the core aims and design of the system and regulatory requirements.

17.3 System operators should not adopt discriminatory pricing. Fees paid by a merchant should not be dependent on whether the merchant also accepts other retail payment instruments or not.

17.4 Relevant cardholders' fees and charges should be transparent to cardholders and service agreements with merchants should specify clearly the relevant fees and charges chargeable to merchants.

OVERSIGHT REQUIREMENTS

18)   Data Collection

18.1   System operators should submit to the HKMA, to the extent permitted by law, at such intervals and in such manner as specified by the HKMA, statistics such as the number of cards issued and in circulation, the total volume and value of transactions, the number of terminal facilities, system performance and relevant financial information. System operators may also be reasonably required to provide certain information to the HKMA on an ad hoc basis to facilitate its oversight of the compliance of the system operators with the Code. Such information, if considered useful for payment system research, may be published by the HKMA in an aggregate form.

18.2   System operators should inform the HKMA of major decisions that may affect the safety and efficiency of the system, such as changes in the rules and procedures that may affect the risk profile of the system operators, merchants and cardholders, fees and charges, etc.

19)   Compliance

19.1   System operators are expected to perform a self assessment of compliance and submit their report to the HKMA annually. System operators may also be required to conduct third party assessment on specific risk areas suggested by the HKMA where appropriate. The internal auditors of the card issuers, merchant acquirers and system operators should check their compliance with the Code in their on-going audits.