Octopus Cards Limited

Report on the Independent Review under Section 59(2) of the Hong Kong Banking Ordinance

July 2007

PRICEWATERHOUSECOOPERS

TABLE OF CONTENTS **PAGE**

Note: Provided under separate cover: "Addendum to the Independent Review under Section 59(2) of the Hong Kong Banking Ordinance: Detailed Findings and Recommendations"

1. INTRODUCTION

As a result of the recent incidents which involved failure to add value to Octopus cards at add-value machines within certain MTR and KCR stations using EPS and where the concerned Octopus cardholders' bank accounts were also debited, we were commissioned by Octopus Cards Limited ("OCL") to conduct a review under Section 59(2) of the Hong Kong Banking Ordinance focusing on certain specific areas of OCL's operations as set out in our engagement letter dated 1 March 2007.

This report sets out the key findings and recommendations from our review and comprises the following sections:

- Overview of OCL's history and operations;
- Scope of work and review procedures performed;
- Findings and recommendations; and
- Assignment limitations and use of this report.

Due to the potentially sensitive nature of certain commercial, technical and security related information contained in the detailed findings and recommendations arising from our work, such detailed findings and recommendations are set out in an addendum to this report entitled "Addendum to the Independent Review under Section 59(2) of the Hong Kong Banking Ordinance: Detailed Findings and Recommendations" ("the Addendum"). This report and the Addendum together comprise the full details of the findings and recommendations from our work.

2. OVERVIEW OF OCL'S HISTORY AND OPERATIONS

OCL (formerly known as Creative Star Limited) was established in 1994 to oversee the development and implementation of a contactless smartcard system in Hong Kong targeted to provide a more convenient method of fare payments for public transportation. It was formed as a joint venture by five major public transportation companies in Hong Kong - MTR Corporation ("MTRC"), Kowloon-Canton Railway Corporation ("KCRC"), Kowloon Motor Bus, Citybus, and Hongkong and Yaumatei Ferry. In January 2001, the shares held by Hongkong and Yaumatei Ferry in the company were transferred to New World First Bus and New World First Ferry. In the same year OCL was transformed from its previous non-profit making status to a profit making organisation. In 2005, a corporate restructuring took place to cope with the business development needs of OCL and Octopus Holdings Limited was established to become the holding company of OCL.

The Octopus card system is an offline system and is made up of two major components: Octopus cards and Octopus card reader/writers. The Octopus card is based on contactless smartcard technology. Data communication between an Octopus card and an Octopus card reader/writer is protected by security control measures such as data encryption.

The usage of Octopus cards involves two key stages: add value by cardholders through designated channels and the subsequent usage for payment of purchases at participating merchants. To cope with the growth of the business, various add-value channels have been introduced by OCL to facilitate ease of use by cardholders since 1997, which include the following:

- Add-value machines ("AVM") located within MTR and KCR stations (and owned and maintained by them) using EPS and cash (which are referred to as "EPS enabled add-value machines" hereafter);
- Counters ("OCP/OTP") at MTR and KCR stations using cash;
- Automatic Add Value Service through designated bank credit card accounts (which are referred to as "AAVS" hereafter);
- Add-value machines located at car parks and shopping malls (and owned by the respective merchants) using EPS (which are referred to as either "EAVM" or "EPS enabled add-value machines" hereafter);
- Point-of-Sales systems at certain retail outlets using cash; and
- AEON Automated Teller Machines ("ATM") through AEON credit card accounts.

As an offline system, transaction data is initially captured in the Octopus card reader/writer and is uploaded to OCL's back end system (the current version is known as the Octopus Clearing House System and is referred to as "OCHS" or "Octopus System" hereinafter) on a non-real time basis for clearing and settlement purposes. Depending on the nature of their business, different data collection mechanisms are used by different transport operators and merchants. For example, transactions could be uploaded from the transport operators and merchants to OCHS for clearing and settlement purposes via networks or offline handheld devices.

Whilst the Octopus card was introduced initially for transportation fare payments, as a result of its success and popularity amongst the Hong Kong public since its launch in 1997, the scope of its use has gradually expanded to cover a wide range of non-transport related transactions. In 2000, OCL was authorised by the HKMA as a deposit-taking company under the Hong Kong Banking Ordinance and the restriction of having not more than 15% of Octopus card transactions for non-transport transactions was removed. Nowadays, Octopus cards are accepted by over 440 different service providers and merchants for payment of purchases of consumer products and are also used as a means of payment in vending machines, pay phones, photo booths, parking meters, car parks, etc. In addition to payment transactions, Octopus cards are also used for access control at office buildings, residential buildings, schools, etc. According to OCL's statistics, as of today there are over 14 million Octopus cards in circulation and on average 95% of the population of Hong Kong use Octopus cards. Over 10 million transactions are generated from the use of Octopus cards in Hong Kong on a daily basis with an aggregate transaction value of approximately HK$29 billion a year.

As a technology based company and one which outsources certain functions to external service providers (e.g., data processing centre), the high volume of

transactions and the large customer base of the Octopus card business is managed and operated by approximately 170 headcounts.

Reporting to the Board, the Senior Management Group comprising the Chief Executive Officer and other departmental heads is responsible for making all major business and operational decisions for OCL.

3. SCOPE OF WORK AND REVIEW PROCEDURES PERFORMED

Our work was divided into three phases, an overview of which is set out as follows:

Phase 1: Incident review and root cause analysis

- To understand and seek to ascertain possible root causes for the known 571 incidents / affected transactions that occurred between 5 December 2006 and 3 February 2007 (inclusive) as reported by OCL.

Phase 2: Expanded investigation of phase 1 findings and review of the Refund Process developed by OCL for failed add-value transactions using EPS

- To consider whether any evidence exists which might indicate that the overall problem is more extensive than the known 571 incidents (that were previously identified by OCL to have occurred during the period from 5 December 2006 to 3 February 2007) in terms of both time period and range of affected add-value devices;
- To review and seek to identify possible root causes leading to the incidents / affected add-value transactions; and
- To review the processes and procedures for identifying, locating and refunding the Octopus cardholders of the original 571 cases, and comment on the adoption of the same processes and procedures for the unclaimed cases prior to 5 December 2006 for failed add-value transactions using EPS (i.e., transactions arising from EPS enabled add-value machines located at MTR and KCR stations) and prior to 18 February 2007 for failed add-value transactions using EAVM (i.e., transactions arising from EPS enabled add-value machines located at car parks and shopping malls).

Phase 3: Review of OCL's technology and operational risk management processes and procedures

- To review OCL's technology and operational risk management processes and procedures in the following selected areas:
  - IT system and infrastructure change management
  - Management and oversight of outside service providers and merchants
  - Problem and PR handling management
  - Consumer protection management

Our review was conducted through interviews with OCL senior management and

staff and certain relevant third parties; review of relevant documentation and procedures manuals; review of selected internal audit reports and OCL's internal investigation and reconciliation reports; performance of certain data reconciliations, analytics and log analysis procedures; and observation and performance of certain technical simulations. Our work was based on obtaining an understanding of the relevant processes and control procedures in operation during the period from 5 March 2007 to 15 June 2007 through performance of the above review procedures.

4. FINDINGS AND RECOMMENDATIONS

In accordance with the scope of work and based on the review procedures performed by us as outlined above, the following notable findings and recommendations came to our attention:

Incident Review and Root Cause Analysis

Based on the review procedures performed, no evidence was identified to suggest that add-value channels other than EPS (inclusive of those located at MTR/KCR stations, car parks and shopping malls) were affected (i.e., identified to have caused failed add-value transactions to occur and where the concerned Octopus cardholders' selected bank account was also debited).

In respect of the add-value failure incidents using EPS, we noted that the original 571 incidents, which occurred between 5 December 2006 and 3 February 2007 (inclusive) as previously reported by OCL, were not the direct result of an isolated incident or event. Rather, incidents of add-value failures using EPS were identified in all periods (and in patterns which are statistically consistent with our root cause analysis findings) where relevant data was available to us (i.e., since January 2000).

Evidence exists to indicate that the root causes leading to the add-value failures using EPS, where value was deducted from the cardholders' selected bank account but the corresponding amounts were not added to the Octopus card, are associated with a number of technical design issues in certain components within the Octopus EPS add-value process. These are described in more detail below.

Given the technical nature of these issues, it is first necessary to provide an overview of the Octopus EPS add-value process itself. The complete Octopus EPS add-value process requires the interaction of a number of complex and interdependent technology components (both hardware and software) which were developed, implemented and maintained by a number of different parties including OCL. In addition, there are also different models of add-value machines which use EPS and different add-value channels using EPS. In general, the different technology components include the following:

- The Octopus card which stores the actual value and has certain processing capabilities;
- Card reader/writer located within the add-value machine to read from and write instructions (including value) to the Octopus card;

- Electronic Funds Transfer module ("EFT module") located within the EPS enabled add-value machine that issues instructions to the host system at EPS Company (Hong Kong) Limited ("EPSCO") to deduct value from bank accounts or to reverse such transactions. The EFT modules are developed by third party suppliers and certified by EPSCO;
- Communications and networking systems that manage the data transmission between different components (e.g., between the various components within the EPS enabled add-value machine, and between the add-value machine and the EPSCO host system);
- Software located within the EPS enabled add-value machine responsible for issuing instructions to add value to an Octopus card; and
- Systems located within the EPS enabled add-value machine responsible for managing information / messages displayed to the cardholder.

It should be noted that the proper functioning of the complete Octopus EPS add-value process can also be affected by certain operational circumstances (e.g., network interference affecting electronic transmissions) and that certain safeguards (e.g., issuing payment reversal instructions) were designed into various components to address some (but not all) of these operational circumstances.

Our root cause analysis identified the following technical design issues to which the majority of the add-value failures using EPS that have been identified are attributable:

- One type of certified EFT module responsible for communicating with the EPSCO host system can malfunction and fail to send the payment reversal instruction after a short time period of network disconnection and reconnection between the EPS enabled add-value machines located in MTR stations and the EPSCO host system. Whilst such network disruptions are part of normal operating conditions and do occur from time to time, the design of this type of EFT module does not adequately cater for such conditions. Under such circumstances, any pending payment reversal instructions that might have been stored in the EFT module prior to the network disruption would be lost; and
- The host system at EPSCO does not process reversal requests from add-value machines for failed add-value transactions received after the EPSCO system's daily cut-off time but where the associated payment debit instruction was received and processed prior to the daily cut-off time.

Given the complexity and nature of the Octopus EPS add-value process, isolated failures with add-value transactions could still occur from time to time, and therefore, there is currently a degree of reliance placed on cardholders to report such failures to OCL if they become aware of them. Reported failures are dealt with under OCL's established refund policy and procedures. However, we also identified issues in the design of certain messages displayed by the add-value machines which could inadvertently be misleading to, or misinterpreted by, the cardholder. In particular:

- The EPS enabled add-value machines at car parks and shopping malls display a message that the transaction was successfully completed even if the cardholder cancels the add-value process or prematurely removes the Octopus card from the EPS enabled add-value machine during the add-value process. In such cases, value would not have been added to the card but the corresponding amount would have already been deducted from the selected bank account; and
- In situations where the selected bank account has already been debited through EPS but the corresponding value could not be added to the Octopus card for various technical and operational reasons such as a communication failure between the different components within the EPS enabled add-value machine, a screen message is displayed indicating either that the transaction was rejected or not completed, and that also instructs the customer to contact the Customer Service Centre in the MTR/KCR station (if it was the latter case). However, this could still lead the cardholder to incorrectly assume that the add-value transaction did not take place and that no money was deducted from the relevant bank account.

Through a detailed analysis of logs that were recorded and maintained during the period of 5 December 2006 to 3 February 2007, it was identified that approximately 80% of the population of failed add-value transactions using EPS[1] that occurred during this period can be attributed to the identified root cause of the malfunctioning of one type of certified EFT module (i.e., with regard to the failure to send a payment reversal instruction after a short time period of network disconnection and reconnection) and approximately 84% to a combination of all the identified and attributable root causes respectively. Whilst one-to-one mapping of records could not be conducted (due to the unavailability of logs within the respective EPS enabled add-value machines) for the remaining 16% of the failed add-value transactions such that they cannot be directly attributed to any of the identified root causes, possible explanations for the remaining 16% of the failed add-value transactions using EPS could be as follows:

- It appears to be likely that 4% of the remaining 16% (i.e., those originating from the EPS enabled add-value machines located at car parks and shopping malls) were due to the above identified root cause of displaying a potentially misleading message when the cardholder cancels the add-value process or prematurely removes the Octopus card from the EPS enabled add-value machine during the add-value process; and
- It is possible (but not verifiable) that 5% of the remaining 16% (i.e., those originating from MTR based EPS enabled add-value machines) and a further 7% (i.e., those originating from KCR based EPS enabled add-value machines) are due to the use of the system 'reset' function of the EPS enabled add-value machines. Currently, when the system 'reset' function of an EPS enabled add-value machine is manually triggered during system maintenance or whenever an EPS enabled add-value machine malfunctions and a manual reboot of the machine is required, any payment reversal instructions that were

[1] The total number of failed add-value transactions using EPS identified for the period between 5 December 2006 and 3 February 2007 are 709, which consists of 571 incidents as previously reported by OCL, 27 failed EAVM transactions, and 111 cases which were already refunded through OCL's existing customer refund policy and procedures.

previously stored in the memory buffer of the EFT module would be automatically removed. We noted that the operations manual for the EPS enabled add-value machine does not currently contain a detailed explanation or instructions on how the system reset function should be used or the implications of the same on any payment reversal instructions that may have been stored in the EPS enabled add-value machine when the system reset function is triggered.

The technical design issues noted above are collectively symptomatic of a more fundamental root cause which is the lack of thorough and coordinated unit, certification and integrated end-to-end testing over the complete Octopus EPS add-value system and its components[2]. This is especially critical in such a complex system involving a number of different parties.

Despite the above, errors can occur due to certain inherent technology characteristics associated with complex commercial systems of this type. Whilst no evidence was identified to suggest that these issues are linked to any of the identified failed add-value incidents using EPS, they cannot be absolutely ruled out as a potential cause as not all add-value failures can be directly attributed to the identified root causes.

We recommend that OCL consider implementing certain enhancements (working in conjunction with relevant third-parties where necessary) to address the problems arising from the identified root causes, the key ones of which are as follows:

- rectifying the malfunction in the relevant certified EFT module and obtaining appropriate re-certification;
- enhancing the error logging and/or handling capabilities between the various software components of the EPS enabled add-value machines and with the EPSCO host system;
- incorporating suitable unique identifiers (e.g., Octopus card ID) in the relevant EPSCO transaction file and using such identifiers to enhance reconciliation procedures to facilitate improved and more proactive identification of potential failed add-value transactions; and
- improving the clarity of messages displayed at EPS enabled add-value machines to the customer during the add-value process.

Our detailed recommendations to address or mitigate the risks associated with the identified root causes as well as other weaknesses have been provided to OCL. We recommend that OCL management study and evaluate our recommendations thoroughly, and implement accordingly. Further, we would recommend that the OCL Board consider treating the satisfactory implementation of these recommendations as a key factor in any decisions regarding the resumption of the Octopus EPS add-value service.

[2] Components are unit tested and/or certified or type approved by the respective responsible party in relative isolation.

Review of the Refund Process for Add-Value Failures Using EPS

As a result of the Octopus EPS add-value failure incidents, OCL developed a process which was used to identify and refund the 571 cases which occurred between 5 December 2006 and 3 February 2007 as previously reported by OCL. OCL management proposed that this process ("the Octopus EPS Refund Process") be adopted to identify further earlier cases of failed add-value transactions using EPS for the purpose of identifying potential cases for refund. We reviewed the Octopus EPS Refund Process and noted that this process does enable OCL management to use internally available information to estimate potential failed EPS related add-value cases to form the basis of making refunds. We have also provided certain recommendations to OCL management to enhance this process.

Based on our review procedures performed, we identified a number of findings pertinent to this process, the notable ones of which are highlighted below:

- The Octopus EPS Refund Process allows OCL management to identify potential failed EPS related add-value cases for the purpose of making refunds. However, given the inherent data limitations, this process does not necessarily guarantee that all failed EPS related add-value transactions are identified;
- OCL could not perform the matching process for a limited number of days during the period between 1 January 2000 and 4 December 2006 where we understand that the relevant datafiles (either the Octopus System or EPSCO datafiles) were missing or for periods prior to 1 January 2000 because OCL's policy is to retain records for 7 years based on OCL's assessment of the relevant statutory requirements. The lack of information on individual transactions means that OCL will be unable to make any refunds under the Octopus EPS Refund Process for failed add-value transactions using EPS which occurred in such periods; and
- The list of possible refund cases also includes certain cases which may not qualify for a refund (i.e., resulting in possible cases of over-refunding) but due to data quality issues have been retained on the list because their validity cannot be fully ascertained. These include: (i) certain successful add-value transactions which were not deducted from the list of refunds because there was insufficient data for these transactions to be matched to a specific add-value record in the relevant EPSCO datafiles; and (ii) no deductions were made from the list of refunds for cases already refunded during the period from 13 January to 31 July 2006 because the documentation relating to these refund cases had been previously destroyed for data privacy considerations. The amounts related to these two situations are approximately HK$700K and HK$140K respectively.

Subject to the above data limitations, we understand that OCL has identified through the Octopus EPS Refund Process a total of approximately 15,300 potential failed add-value transactions using EPS amounting to approximately HK$3.7 million between 1 January 2000 and 4 December 2006 which could be refunded. These figures incorporate several minor adjustments following implementation of our recommendations in this area.

We have been advised by management that OCL will initiate steps and make the relevant refunds accordingly.

Review of OCL's Technology and Operational Risk Management Processes and Procedures

We reviewed OCL's technology and operational risk management processes and procedures in the areas set out below. This included taking into consideration the relevant requirements set out in the various codes of practice and the Supervisory Policy Manuals ("SPMs") issued by the HKMA, namely the Code of Banking Practice, the Code of Practice for Multipurpose Stored Value Card Operation, and the SPMs on General Risk Management Controls ("IC-1"), Operational Risk Management ("OR-1"), Technology Risk Management ("TM-G-1"), Outsourcing ("SA-2") and Complaint Handling Procedures ("IC-4"):

- IT system and infrastructure change management
- Management and oversight of outside service providers and merchants
- Problem and PR handling management
- Consumer protection management

Based on our review, we identified a number of issues concerning OCL's operational and technology risk management processes and procedures and system of internal control. In response to these findings and observations, we have made a number of recommendations for OCL's consideration to enhance the robustness and effectiveness of its internal control system for managing its technology and operational risks and addressing certain issues relating to consumer protection. These issue observations and recommendations are highlighted below:

- **Greater ownership in overseeing and managing the implementation and integration of systems and critical components of the Octopus system provided by third party providers should be taken up by OCL.**

  The development and maintenance of various front-end devices or modules supporting the Octopus add-value process requires the involvement and collective efforts of OCL and other third party service providers. From our discussions with OCL management and personnel, and in view of the various identified root causes leading to the add-value failure incidents using EPS, it appears that OCL has taken a view that OCL and these third party service providers are each responsible for the proper functioning of their respective individual components supporting the Octopus system. OCL has placed heavy reliance on the third party service providers' internal quality assurance process and agreed-upon protocols/structures and has not defined or put in place an appropriate oversight process with regards to managing the implementation and integration of systems and critical components developed by such third parties. We believe that this view has resulted in instances of insufficient impact analysis being carried out and the lack of a thorough and coordinated unit, certification and integrated end-to-end testing process.

  We recommend that OCL take greater ownership in overseeing and managing

the implementation and integration of systems and critical components developed by outside third parties. Sufficient due diligence and impact analysis should be carried out by OCL against the work performed by such third parties prior to placing reliance on them. In this regard, an appropriate level of risk assessment and impact analysis should be conducted by OCL with regard to all changes implemented by OCL and other related third parties which are deemed to be critical to OCL's business operations. In addition, OCL should also develop and adopt a more integrated testing approach for system implementation and change management activities, and enhance the controls over the program migration process, data patching activities and data backup and restoration procedures.

- **A clearer identification of OCL's oversight responsibilities over certain outside parties which form an integral part of OCL's business operations should be established.**

  As an Authorized Institution, OCL is responsible for retaining ultimate accountability for outsourced activities and implementing effective procedures for monitoring the performance of, and managing the relationship with, such outsourcing service providers. Based on our discussions with OCL management and personnel, we noted a pervasive view within OCL that outside service providers ("OSPs")/merchants providing add-value services for and on behalf of OCL are OCL's business partners and that each party is, therefore, largely responsible and accountable for its own acts and conduct. The monitoring and oversight procedures put in place by OCL over such OSPs/merchants were developed in the context of this view and, therefore, tend to focus more on the commercial aspects (e.g., prompt monetary settlement by these parties). As a result, the existing procedures do not enable OCL to effectively oversee all relevant key aspects of the conduct / activities of the OSPs/merchants which are critical to OCL's business operations. Any performance failures caused by these OSPs/merchants could significantly increase the operational, legal and reputational risks facing OCL.

  We recommend that OCL put in place a process of assessing the criticality and risks (encompassing, at a minimum, operational, legal and reputational risks facing OCL) of operations and activities performed by outside third parties, and clearly identify and define its oversight responsibilities over the same taking into account the relevant regulatory principles/guidelines underlying outsourcing arrangements. In addition, a thorough review of the existing monitoring procedures and mechanisms should be carried out by OCL to ensure that they are (i) in line with the re-defined oversight responsibilities of OCL; (ii) in compliance with the relevant requirements set out in the HKMA SPM on Outsourcing (i.e., SA-2); and (iii) adequate for the discharge of OCL's responsibilities. In this regard, terms and conditions included in the service agreements with OSPs/merchants should be enhanced, monitored and enforced by OCL. OCL should discuss with MTRC and KCRC to help ensure that appropriate operational manuals and/or procedures are prepared and agreed to address the maintenance requirements of AVMs located at MTR and KCR stations and also reduce the risk associated with the potential mis-use of the system 'reset' function of the

EPS enabled add-value machines. In addition, OCL should formalise the existing policies and procedures in tracking and handling of incidents raised by OSPs/merchants.

- **An integrated problem management framework should be established.**

  Within OCL, the approach and procedures adopted for incident response, management and reporting among different departments are different, and the definitions and delineation of roles and responsibilities for the handling of incidents in each department have not been formalised or fully identified. In addition, an effective central oversight process enabling better identification and consideration of shared or underlying common issues has yet to be put in place. As a result, the implications of and root causes relating to an incident have not always been fully evaluated or adequately identified in the past. The establishment of an integrated problem management process will significantly improve OCL's ability to manage incidents proactively and in a holistic manner.

  We recommend that OCL review and enhance its existing problem management process by (a) assessing the sufficiency of information captured in the exceptions reports received; (b) establishing a formal definition of 'incidents' triggering different escalation requirements; (c) establishing a clearer delineation of roles and responsibilities amongst individual departments and harmonising procedures where possible; and (d) creating a central oversight function/process to facilitate the analysis of incidents identified and responses to the same in a holistic manner, i.e., cross departmental. In this regard, communication of issues by the Operations Department to other departments and among different departments within OCL for follow-up actions should be enhanced. Evaluation of potential issues underlying cardholders' enquiries and complaints and information captured in the Refund Databases should be enhanced and better utilised. The current approval process with regards to the issuance of press releases should also be enhanced.

- **A more appropriate balance should be struck between OCL's and cardholders' interests in the evaluation of business and operational issues.**

  Based on our discussions with OCL management and review of documentation made available to us, including reports and meeting minutes which documented various business and operational issues, it appears that the primary focus of OCL in evaluating business and operational issues has been on their potential commercial implications to OCL. As a result, measures which may have enhanced consumer protection (e.g., alternative processes to refund unclaimed values) do not appear to have always been sufficiently evaluated or considered by OCL prior to the EPS related add-value failure incidents.

  OCL's large cardholder base (around 14 million) and its significance to the Hong Kong general public warrants consideration of consumer protection issues and developments affecting OCL to be included as part of the standing

agenda of the Board. We therefore recommend that OCL Board/senior management re-assess the extent to which cardholders' interests are being considered in the evaluation of business and operational issues of OCL, and appropriate management processes (e.g., dedicated consumer protection oversight function, liaison with consumer protection groups, etc.) be considered to enable such information to be collected, assessed, and reported to the Board. The outcome of such an assessment should include developing a more thorough understanding of the position and interests of OCL's cardholders as depositors of OCL. Subject to this assessment, OCL should revise where necessary its operating policies and processes or introduce new practices to better address cardholders' interests. In this regard, we recommend that OCL establish a more proactive process and procedures for identifying, locating, and handling of Octopus cardholders who have unclaimed values, and revisit the record keeping policy on refunds to cardholders. OCL should also enhance cardholders' awareness of their rights and responsibilities in the usage of Octopus cards, and consider assigning additional call centre resources for handling lost card reports to enhance customer services.

- **A review should be performed to identify those areas where governance structures and processes could be developed or enhanced to better support OCL's business going forward.**

  OCL holds a unique position in Hong Kong as it:

  - has extensive reach and day-to-day interaction with a large base of customers;
  - operates with leading-edge technological systems that form a key part of Hong Kong's electronic payments system;
  - has a broad network of service providers and business relationships; and
  - is an Authorized Institution under the Hong Kong Banking Ordinance.

  This status is substantially different from that which existed at the time when it was first formed (as Creative Star Limited) to operate a contactless smart card system for automatic fare collection for Hong Kong's public transport systems. Over time, OCL has grown substantially from its transport origins to become an integral part of Hong Kong's electronic payment system and a regulated institution supervised by the HKMA.

  In contrast, we noted that some of its governance and controls structures do not appear to have evolved commensurately. More specifically, for an organisation of OCL's size and status, certain important governance and control elements which play an important part in OCL's system of internal control and which are relevant to the add-value process require improvement:

  - **IT governance framework**: Whilst we noted that an IT Steering Committee, which consists of the various department directors and the CEO, is in place to provide oversight of the company's IT strategy and plan, with reference to the various HKMA SPMs, in particular TM-G-1, we believe that the coverage of OCL's existing IT policies, procedures and

guidelines should be enhanced with regards to security management, system development and change management, information processing, communication networks and management of technology service providers. In addition, we recommend that a more comprehensive IT governance framework be developed and approved by the Board and implemented and monitored on an ongoing basis.

- **Internal audit**: Whilst OCL has an established internal audit function (which reports to the Audit Committee), through examining a sample of internal audit reports (i.e., those related to EPS related add-value issues), it appears that the majority of audit findings were assessed by the Internal Audit Department primarily from a financial risk perspective. Other aspects such as regulatory and reputation risks, impact to other stakeholders, cardholders' interests, etc. do not appear to have been a key focus of the Internal Audit Department. The existing approach of the Internal Audit Department could be revisited to better align their focus with the broader range of risks facing OCL in order to ensure that a more holistic/balanced approach is undertaken going forward.
- **Compliance duties and responsibilities**: OCL is an Authorized Institution regulated by the HKMA and is subject to various requirements stipulated in the Hong Kong Banking Ordinance, the codes, guidelines, circulars and SPMs issued by the HKMA from time to time. The Board is responsible for ensuring that OCL's operations are properly controlled to help ensure compliance with these regulatory requirements. Whilst we note that compliance duties are currently shared by different departments, there is no centralised monitoring mechanism in place (e.g., to assist with the interpretation and understanding of regulations, performance of regular compliance surveillance testing, etc). Given OCL's scale of operation and nature of its business, we recommend OCL to re-assess the existing compliance framework and approach including the adequacy of resources assigned to the handling and monitoring of compliance requirements. OCL should also consider the need for a dedicated compliance committee and function responsible for the development of formalised compliance related policies and procedures to address OCL's obligations.

The above issues came to our attention during the course of our work. We are of the view that these represent more pervasive issues that could have a bearing on our more detailed findings and recommendations and, therefore, warrant OCL senior management's and the Board's attention. We recommend that a review of this area be carried out to identify those governance structures and processes that could be developed or enhanced to better support OCL's business going forward. This will also help to ensure the effective and sustainable implementation of the recommendations identified from this review.

Our review was primarily aimed at OCL's add-value process and technology and operational risk management processes and procedures. We have not performed a review of other aspects of OCL's business or systems. However, during the course of our review of OCL's technology and operational risk management processes, and other than those issues already identified in this

report, no other systemic issues comparable to the nature and scale of the add-value process issue came to our attention.

5. ASSIGNMENT LIMITATIONS AND USE OF THIS REPORT

The nature of certain IT/system errors or problems in any complex IT environment is that they may not always be repeatable and observed. Despite the fact that our review procedures were designed to review and seek to identify possible root causes and report these accordingly, we cannot guarantee that: i) all attributable root causes leading to the recent incidents of failure to add value to Octopus cards at add-value machines within MTR/KCR stations, car parks and shopping malls etc. have been identified; or ii) all incidents of failure to add value have been completely identified.

The scope of work performed by us was determined by the purpose of the engagement and the requirements of the HKMA at the time the review was commissioned. Accordingly, the report and/or any extracts or parts thereof should not be regarded as suitable for use by any other persons or for any other purpose. PwC accept no responsibility or liability in respect of the report or any extracts or parts thereof or references made with respect thereto to persons other than OCL.

The report relates to certain matters as at 15 June 2007. Events may occur or may have occurred since that date and/or since the date of the report, which, had they come to light prior to the date of the report, may have affected the conclusions reached or information contained in the report or any extracts thereof. Control procedures are subject to inherent limitations, and accordingly, errors, irregularities or system control weaknesses may occur and not be detected. In addition, the projection of any conclusions based on our findings arising from this review to future periods is subject to the risk that changes will be made to systems and/or controls to allow for development of business or other requirements. The validity of projecting any conclusions in light of the possibility of such changes must be considered.

By its nature, this report includes sensitive and confidential information, the distribution of which should be carefully controlled. This report is intended for the sole use of OCL to file with the HKMA in accordance with the HKMA's requirement under Section 59(2) of the Hong Kong Banking Ordinance, and to provide a copy to the independent advisor, Professor Andrew Chan, but without liability to them on our part and for their internal use only.

This report may not be provided by OCL to other third parties (other than OCL's board of directors and shareholders of OCL's immediate holding company i.e., Octopus Holdings Ltd.) for any other purpose without our prior written consent, and that we accept no responsibility or liability in respect of this report or any extracts or parts thereof or references made with respect thereto to any party other than OCL.

We understand that you may wish to make reference to our work or this report in certain public documents. We will need to review and approve such public

documents before they are published and you agree to obtain our prior written permission. In the event that you wish to publish certain parts or extracts of our report in isolation, OCL shall make a statement accompanying the extracts from the report that the full report is not being published and we will need to review and approve such extracts before they are published.