Deloitte
德勤

Octopus Cards Limited

26 November 2010

Enterprise Risk Services

Contents

Acronyms

A-card	Anonymous Octopus Card
AAVS	Automatic Add Value Service
AC	Audit Committee
AIA	American International Assurance Company Limited
AIU	American International Underwriters Limited
Board	Board of Directors
CEO	Chief Executive Officer
CIGNA	CIGNA Worldwide Insurance Company
Cimigo	Cimigo Limited
CPP	Card Protection Plan Limited
CRM	Customer Relationship Management
DAR	Data Access Request
DCR	Data Correction Request
DTT/HK	Deloitte Touche Tohmatsu in Hong Kong
eDM	Electronic Direct Mailing
HKID	Hong Kong Identity Card
HKMA	Hong Kong Monetary Authority
IAD	Internal Audit Department
INED	Independent Non-executive Director
LegCo	Legislative Council of the Hong Kong Special Administrative Region
McKinsey	McKinsey & Company
MI	Magazine International (Asia) Limited
NED	Non-executive Director
OCL	Octopus Cards Limited
OCT	Octopus Connect Limited
Octopus Group	Octopus Holdings Limited and its subsidiaries
OHL	Octopus Holdings Limited
ORL	Octopus Rewards Limited
P-card	Personalised Octopus Card
PCA	Privacy Compliance Assessment
PCPD	Office of Privacy Commissioner of Personal Data
PDPO	Personal Data (Privacy) Ordinance
PIA	Privacy Impact Assessment
RMC	Risk Management Committee
RMD	Risk Management Department
SAM	Sales and Marketing Department
SDR	Strategy, Development and Risk Management Department
T&C	Terms and Conditions
TNS	Taylor Nelson Sofres Hong Kong Limited

Important Notes to Reader

Our report is solely prepared for the purpose set forth in Section 1 of this report (the "Report") and for OCL information, and is not to be used for any other purposes. Our Report will not include any representation as to the quality or performance of the OCL's goods or services nor their fitness or suitability for any customer's intended purpose.

In preparing our Report, we have relied upon the representations made to us by the management, officers and staff of OCL and on the materials made available to us for the purposes of the Assessment. OCL's management warrants that the information provided and materials made available to us are correct to the best of their knowledge and belief and that there will be no other information the omission of which may cause us to be misled or which may appear to be misleading.

Our work does not entail us performing detailed tests of transactions to the extent that would be necessary to disclose all defalcations and irregularities which may exist. Accordingly, reliance should not be placed on our Report to disclose all such matters.

The matters raised in this Report are only those that came to our attention during the course of our field visit. They are not necessarily a comprehensive statement of all the weaknesses that may exist relating to OCL or all the improvements that could be made. The recommendations for improvement that we make should be assessed by OCL for their full commercial and cost implications before they are implemented.

This Report does not constitute either an audit or review in accordance with the Hong Kong Institute of Certified Public Accountants or with any other auditing standards and, consequently, no such assurance is expressed. Your attention is drawn to Section 5 of this Report for the limitations of our Assessment.

We do not assume responsibility towards or accept liability to any other person for the contents of this Report. For the avoidance of doubt, all duties and liabilities (including without limitation, those arising from negligence) to any third party (being any party who is not a contractual party to the engagement letter pursuant to which this Report is issued) is specifically disclaimed.

Except for internal use or otherwise mentioned above, if OCL intends to publish or reproduce our Report or any part thereof in any document (including electronic formats or other media), or otherwise make reference to DTT/HK in a document (including electronic formats or other media) that contains other information, OCL agrees that prior to making any such use of our Report, or reference to DTT/HK, to (1) provide us with a draft of the document to read and (2) obtain our approval for the inclusion or incorporation by reference of our Report, or the reference to DTT/HK, in such document before the document is published and distributed.

1. Introduction

Following the public concern regarding the sharing of Octopus cardholders' personal data with third parties, DTT/HK were appointed by OCL and approved by HKMA to conduct an independent assessment under section 59(2) of the Hong Kong Banking Ordinance.

This Report sets out the key findings and recommendations from our Assessment and comprises the following sections:

- Objective;
- Scope of work;
- Fieldwork period;
- Limitations;
- Statement of responsibilities; and
- Findings and recommendations.

2. Objective

The objective of the Assessment is to report under section 59(2) of the Banking Ordinance (Chapter 155 of the Laws of Hong Kong) in respect of OCL's processes and practices for handling Octopus cardholders' personal data, during the period as set out in Section 3 of this Report, in the context of the requirements of:

- The PDPO (Chapter 486 of the Laws of Hong Kong) and applicable codes and regulations pursuant to the PDPO; and
- The following relevant guidelines:
  - the Supervisory Policy Manual module on Corporate Governance of Locally Incorporated Authorised Institutions (CG-1) issued by HKMA;
  - the Code of Banking Practice; and
  - the Code of Practice for Multi-Purpose Stored Value Card Operation.
  (collectively known as the "Guidelines")

DTT/HK was not engaged to and did not provide any legal advice or conduct any legal review of any of OCL's documents, records or policies. We were also not engaged to provide any legal opinion on whether OCL's policies and procedures comply with PDPO or the Guidelines.

3. Scope of Work

The scope of the Assessment covered the following areas of focus for the period from 15 July 2002 (the date when customers' personal data were first provided to third parties (including by any related companies of OCL)) to 4 August 2010 (the date of commencement of this Assessment):

(a) Establishing whether and if so, which third parties (excluding service providers for outsourced operations e.g. for manning of customer service hotlines, and public authorities e.g. by Police) had access to or received from OCL any Octopus cardholders' personal data, and what personal data was passed to these third parties, if any;

(b) Establishing what relevant governance structure, policies, procedures and controls were in place to govern the disclosure of Octopus cardholders' personal data by OCL to third parties and to ensure adequate protection of such data in accordance with the abovementioned laws, codes and regulations, including establishing how OCL communicated these policies, procedures and controls to its staff and administered staff compliance with them;

(c) Establishing what due diligence OCL performed in drawing up these terms and conditions (e.g., what legal due diligence was performed, whether appropriate prescribed consent was obtained from cardholders before any personal data was passed to third parties) and how OCL administered compliance by the personal data recipients with these terms and conditions; and

(d) Making recommendations to enhance the effectiveness of any relevant areas and to address any weaknesses identified.

Our procedures performed were set out as follows:

(a) Obtained and inspected relevant contractual agreements signed between OCL and third parties (including any related companies of OCL but excluding service providers for outsourced operations such as for manning of customer service hotlines and public authorities such as the Police), under which any Octopus cardholders' personal data was allowed to be accessed by or was passed to these third parties and identified which third parties had such access and what personal data was accessed and/or shared;

(b) Inquired with relevant personnel of OCL to understand the governance structure, policies, procedures and controls that were in place to govern the disclosure of Octopus cardholders' personal data by OCL to third parties;

(c) Obtained the policies and procedures, and available documents, records, information and audit trails to consider whether procedures for data protection were established in accordance with the Guidelines;

(d) Inspected available documents, records, information and audit trails to consider whether OCL communicated these policies, procedures and controls to its staff and administered staff's compliance with them;

(e) Inquired with relevant personnel of OCL and inspected available documents, records, information and audit trails to consider the due diligence procedures performed by OCL in establishing terms and conditions in the contractual agreements between OCL and recipients of personal data;

(f) Inquired with relevant personnel of OCL and inspected available documents, records, information and audit trails and to consider the procedures performed by OCL to administer compliance by the recipients of personal data with terms and conditions in the contractual agreements between OCL and the recipients; and

(g) Based on the above-mentioned procedures performed, identified weaknesses, if any, and assessed the impact of the identified issues and made recommendations for improvement of relevant areas.

Our work does not constitute an audit, or a review, or an assurance engagement in accordance with Hong Kong Standards on Auditing, Hong Kong Standards on Review Engagements, or Hong Kong Standards on Assurance Engagements issued by the Hong Kong Institute of Certified Public Accountants, and therefore, no such assurance is expressed. We do not express an opinion or give any other form of assurance with respect to any matters as a result of our work including, without limitation, concerning the (1) financial information of OCL or any financial or other information, or operating or internal controls of OCL, or its compliance with laws or regulations, taken as a whole, for any date or period, or (2) future operations.

4. Fieldwork Period

This Report covers our fieldwork conducted during the period from 4 August to 8 October 2010.

5. Limitations

5.1 Limitations of Our Scope

Documentations and Records

Since our assessment period covered the period from 15 July 2002 (the date when customers' personal data was first provided to third parties outside OCL) to 4 August 2010, which extended beyond the documentation retention period adopted by OCL, the Assessment was performed based on documentation and records available to us during the course of our fieldwork.

Employees have Short History with OCL

We inspected the documents and records maintained by OCL to obtain an understanding of its policies and procedures for data collection, processing, extraction and purging as well as monitoring of related compliance. However, since many employees were new to OCL at the time of our fieldwork, we were not able to confirm the adoption of the following practices with current staff:

- Process for extracting Octopus cardholders' personal data from OCL's database and for sharing data with third parties before the enhancement of its data extraction process in January 2006;

- Data purging and destruction process conducted by third parties who had access to or received from OCL Octopus cardholders' personal data prior to the enhancement of the Personal & Customer Data Protection and Privacy Policy and Procedures in 2008; and
- Process for monitoring compliance with the confidentiality and personal data protection measures performed by recipients of personal data prior to formal documentation of visits to business partners made by OCL in Onsite Visit reports that were prepared from 2006.

5.2 Limitations of an Entity's Internal Controls

Procedures, systems and internal controls, no matter how well designed and operated, can provide only reasonable assurance of achieving an entity's control objectives. The likelihood of achievement is affected by limitations inherent to procedures and internal controls which are dependent for their effectiveness on the diligence and propriety of those responsible for operating them. The limitations include the realities that human judgment in decision-making can be faulty and that breakdowns in internal controls can occur because of human failures such as simple errors or mistakes. Additionally, controls, whether manual or automated, can be circumvented by the collusion of two or more people or inappropriate management override of internal controls.

We would like to point out that changes in conditions over time and after the period of the engagement may alter the effectiveness of the internal controls and that this Report is prepared solely for the period as specified in Section 3 under this Report. The matters raised in any reports to you are not necessarily a comprehensive statement of all weaknesses that exist or of all improvements that might be made. Recommendations for improvement should be assessed by you for their full commercial implications before they are implemented. Furthermore, because of inherent limitations of any system of control, errors, breaches of law, inefficiencies or irregularities may occur and not be detected.

Moreover, projections of any evaluation of controls for the future are subject to risk that controls may become inadequate because of changes in conditions.

Thus, we will not be in a position to provide assurance as to the day-to-day operation of the procedures and internal controls and, therefore, OCL cannot rely on our reports to give such assurance.

6. Statement of Responsibilities

OCL is responsible for the results of this Assessment, including the final assessment of weaknesses in the internal controls, for the evaluation and determination of which recommendations included in our Report should be implemented and for acting on those recommendations. Furthermore, OCL is responsible for establishing and monitoring a system of internal controls and processes in addressing the risks associated with the compliance with the PDPO and the Guidelines. All decisions in connection with the design and implementation of the internal control and processes and the design and implementation of the related computer systems are the responsibility of, and made by OCL. It is OCL's responsibility to perform all management functions, including all significant decision-making.

DTT/HK did not perform any management functions, make management decisions, or perform in a capacity equivalent to that of an employee of OCL. It is understood and agreed that this Assessment may include advice and recommendations to OCL, but all decisions in connection with the implementation of such advice and recommendations shall be the responsibility of the Management of OCL.

7. Findings and Recommendations

Findings and recommendations are summarised in the following subsections:

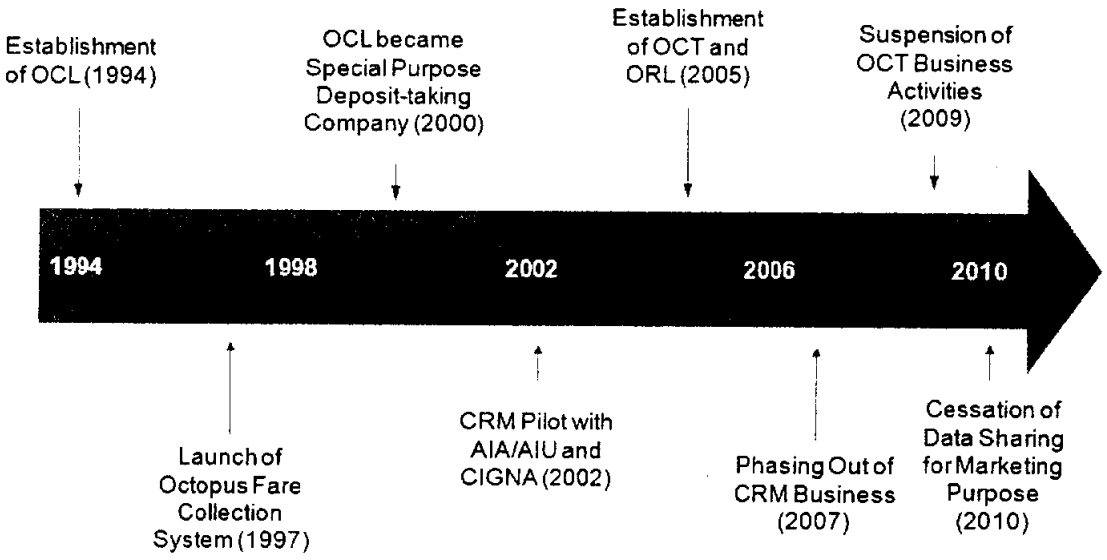
- Chronology of OCL's Development of CRM Business;
- Collection of Personal Data;
- Sharing of Octopus Cardholders' Personal Data with Third Parties;
- OCL's Corporate Governance and Internal Controls;
- Activities Performed by OCL in Complying with PDPO and the Guidelines; and
- Recommendations.

7.1 Chronology of OCL's Development of CRM Business

This section provides the factual findings relating to OCL's CRM business and its control procedures for governing the disclosure of Octopus cardholders' personal data to third parties. Our findings are summarised in the following subsections in chronological order:

- Establishment of OCL;
- Development of CRM Initiative;
- Group Restructuring;
- Launch of Rewards Program;
- Phasing Out of CRM Business; and
- Cessation of Data Sharing for Marketing Purpose

The timeline for the key events relating to OCL's CRM business is summarised as below:



7.1.1 Establishment of OCL (1994)

OCL (formerly known as Creative Star Limited) was established in 1994 as a joint venture by five major public transportation companies in Hong Kong, namely MTR Corporation, Kowloon-Canton Railway Corporation, Kowloon Motor Bus, Citybus, and Hongkong and Yaumatei Ferry to oversee the development and implementation of a contactless smart card system in Hong Kong. OCL aimed to provide a convenient method of fare payments for public transportation.

[Note: In January 2001, the shares held by Hongkong and Yaumatei Ferry were transferred to New World First Bus and New World First Ferry.]

In September 1997, OCL officially launched the Octopus fare collection system. The system allowed commuters to travel across multiple transport modes (i.e. railways, buses and ferries) using a single card in a multi-operator automatic fare collection system.

In order to expand into a wider range of different payment applications, other than for the public transport sector, OCL obtained authorisation to become a special purpose deposit-taking company from HKMA in April 2000.

7.1.2 Development of CRM Initiative (2001 – 2003)

With a view to achieving further business growth, OCL's Board agreed that the management of OCL should explore various options for expanding the role of the Octopus into other services. The management of OCL had identified and launched different types of new Octopus-related products/services associated with the use of the Octopus Card.

The OCL senior management team further conducted a strategic review of OCL's operations and capabilities and the Expansion Strategy for 2003 to 2007 was formulated and approved by the Board as a result. A range of

opportunities were identified and a few categories of businesses were proposed, which included the loyalty program and marketing of goods and services for other organisations.

In April 2002, CEO reported to the Board that OCL and AIA/AIU had explored direct marketing business initiatives for AIA/AIU's insurance products to Octopus cardholders, as well as offering personal accident insurance plans to Octopus cardholders as an introducer. OCL and AIA/AIU entered into an agreement pursuant to which OCL would outsource the telemarketing activities to AIA. AIA/AIU telemarketers then contacted the customers on behalf of OCL. A similar pilot of outsourced telemarketing program with CIGNA commenced in September 2002 in which CIGNA telemarketers contacted the customers on behalf of OCL.

Marketing pilots with AIA/AIU were completed in mid-September 2002 and the pilot program with CIGNA was completed in mid-December 2002. The management of OCL reported to the Board that OCL decided to partner with CIGNA to distribute insurance products to Octopus cardholders in 2003.

7.1.3 Group Restructuring (2002 – 2005)

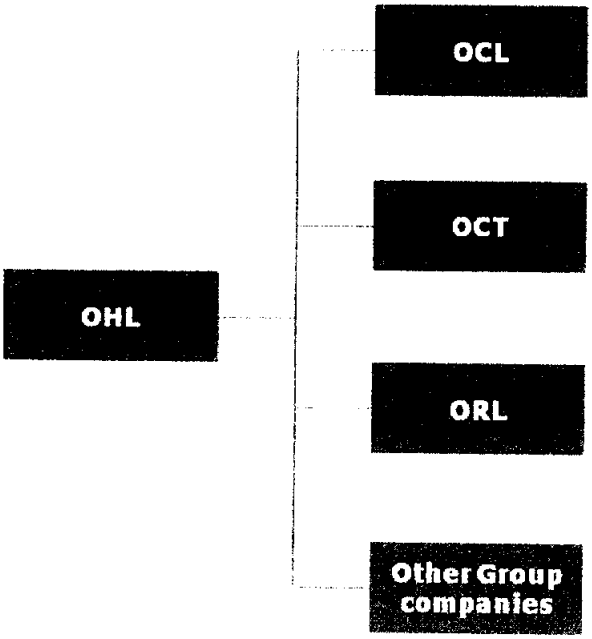
Finance Director of OCL proposed a corporate restructuring plan in May 2002 so as to facilitate the development of the non-payment business. The plan suggested that a spin-off of the non-payment business into separate corporate entities away from OCL's traditional payment business would allow the non-payment business to operate without introducing new dimensions of risk to the payment platform operated by OCL, a Special Purpose Deposit-taking Company subject to HKMA's supervisory guidelines. The Board approved the proposal in May 2002.

In January 2004, OCL launched a "Rewards on the Go" lucky draw program with CIGNA. In this program, customers registered to participate in the lucky draw on OCL's website or by filling in an application form. OCL provided all participants with a free CIGNA insurance policy plan and passed the customer personal data to CIGNA for the provision of such insurance services.

In September 2004, OCL and CPP jointly launched a program introducing the lost card protection service in Hong Kong. OCL acted as the introducer of CPP's lost card protection service, with CPP as the insurance agent to contact the customers on behalf of OCL.

As part of the corporate restructuring, the CRM business was transferred out of OCL. A company was incorporated in February 2003 with the company name changed to OCT in October 2004. The primary objective of setting up OCT was to carry out the data mining activities for OCL as well as other fellow group companies.

OHL acquired all the shares of OCT in October 2005. The corporate restructuring was completed and effective from 21 October 2005. The overall structure of OHL and its subsidiaries ("Octopus Group") after corporate restructuring was as follows:



7.1.4 Launch of Rewards Program (2005)

As described in the OCL Expansion Strategy for 2003 to 2007, an establishment of a loyalty program was one of the expansion ideas proposed by the management of OCL. The loyalty program was again listed as a Board agenda item in the 2004 Strategic Plan.

ORL was incorporated on 23 April 2004 for operating the common loyalty program which subsequently became known as the Octopus Rewards Program. ORL was acquired by OHL in October 2005.

In April 2005, ORL was authorised by the Board to enter into commercial agreements with service providers/direct and indirect merchants of the Octopus Rewards Program.

The operating revenue of ORL would mainly be generated from program administration (i.e. Rewards dollars, issuance and redemption administration fees, fees for marketing communication and program management) and target marketing business (i.e. marketing fees payable by service providers to ORL for tailor-made marketing messages sent to targeted customers on behalf of the service providers). The Octopus Rewards Program was launched on 5 November 2005.

The CRM System was developed and implemented with centralised data warehouse and data mining capability as an alignment with the Expansion Strategy developed in early 2002. The CRM System was further upgraded in 2006 in order to support the target marketing part of the ORL business.

OCL entered into Confidentiality Agreements with OCT and ORL in November 2005. Personal data and transaction records from OCL and ORL were copied daily to the CRM System and stored in segregated database files for data analysis.

OCT would access OCL's customer database for customer data analysis and target marketing support services. OCT would then analyse customer behaviour and extract customer records. ORL would use the result of analysis conducted by OCT and shared ORL customer personal data maintained in its own database with business partners.

7.1.5 Phasing Out of CRM Business (2007 – 2009)

Octopus Group engaged McKinsey to conduct a strategic review project in 2007. One of the findings of this review was that the potential of the data business was limited. McKinsey recommended Octopus Group to consider phasing out OCT and redirecting resources to OCL/ORL to focus on serving Rewards merchants.

In a presentation to the Octopus Board in October 2007, McKinsey stated the following reasons for discontinuing the data business:

1. Difficulty in gaining scale as customer records could not be sold to many parties at any given time;
2. Reputational risk associated with over-using customer information; and
3. Unwarranted diversion of management resources in acquiring and managing major customers.

Following the review by McKinsey, Octopus Group adopted a "Five Year Strategy (2008-2012)" in October 2007 to scale down the data business.

OCT became inactive from 31 December 2009. Its business was discontinued and the remaining headcount and resources were transferred to ORL.

CPP joined the Rewards program of ORL in June 2010 and established an email marketing approach whereby Rewards members would need to request, by clicking a link in the email, that they wished to be called by CPP specifically, where they had interest in the product. Only the contact details of customers expressing an interest in the program would be processed to CPP's call centre for follow-up.

7.1.6 Cessation of Data Sharing for Marketing Purpose (2010)

ORL ceased the business activities with CIGNA and CPP on 9 July 2010 and 15 July 2010 respectively. ORL also suspended the subscription of new Rewards members from 5 August 2010. ORL sent out direct mailing, emails, and SMS messages to the existing Rewards members during the period from 21 July 2010 to 2 August 2010, reminding them that they could opt out of receiving direct marketing materials. Octopus Group is in the process of conducting a data purging exercise in relation to the personal data held by CIGNA and CPP as well as the non-essential personal data collected.

7.2 Collection of Personal Data

7.2.1 Types of Octopus Card

In general, there are two types of Octopus Card:

- A-card; and
- P-card – Octopus Card with Cardholders' name imprinted on the card surface and with data stored inside the card to assist with fare calculation, such as age-based concessions. The OCL customer database also contained the cardholder's personal data.

OCL also introduced AAVS in 1999. When the stored value on the Octopus card reaches zero or negative, or when the remaining value plus the maximum negative value (HK$35) is insufficient to pay for the transaction amount, a pre-selected amount of HK$250 or HK$500 (starting from 2006) will be automatically added to the Octopus card by the Octopus processor (up to once per day), and deducted from the designated credit card account or bank account of the Octopus cardholder.

Until 2004, only P-card holders could apply for AAVS. From 2004, holders of an A-card could also apply for, becoming registered AAVS customers. For these customers, the card continued to contain no personal data but the back-end OCL database would contain such data.

As a result, there are effectively three (3) types of Octopus card in use since 2004 – Anonymous (no personal data on card or in the back-end database); Registered AAVS (no personal data on card but personal data held on back-end database) and Personalised (with or without AAVS) (personal data on the card and on back-end database). The personal data collected through P-card and AAVS are used for business operations of the Octopus card including lost card reporting and processing of automatic reloading for payment through Octopus cards, as well as complying with the "know-your-customer" principle under the Guideline on Prevention of Money Laundering issued by HKMA.

7.2.2 Collection of Personal Data for Octopus Card

According to OCL's "Conditions of Issue of Octopus" which was effective from January 1999, personal data provided by the cardholder could be used by OCL for marketing and promotion of goods and services of OCL and other parties. However, the cardholder could request that his/her personal data not be used for the abovementioned purposes by making a written request addressed to OCL.

In the revised OCL's "Conditions of Issue of Octopus" effective from November 2004, a similar condition was established that the cardholder agreed that his/her personal data could be used by OCL for marketing of goods and/or services by OCL, OCL's subsidiaries and affiliates or any of the selected business partners. The cardholder had the right to request OCL not to use the personal data for direct marketing purposes by making a written request or through the customer hotline.

7.2.3 Collection of Personal Data for Octopus Rewards Program

As stipulated in the Terms and Conditions for Octopus Rewards Program and on the Rewards Program Registration Form since the launch of program in 2005, by signing the registration form, the applicant would agree that ORL and its subsidiaries/affiliates and other business partners might provide marketing services to the registrants (i.e. members). The members could opt out of receiving direct marketing materials by calling a hotline, applying through Octopus' website or in writing.

7.3 Sharing of Octopus Cardholders' Personal Data with Third Parties

This section describes the types of direct marketing activities performed by OCL, what third parties (including any related companies of OCL but excluding service providers for outsourced operations e.g. for manning of customer service hotlines, and public authorities e.g. Police) had access to or received from OCL any Octopus cardholders' personal data, and what personal data was passed to these third parties.

7.3.1 Electronic Direct Mailing ("eDM") sent by OCL

During 2002-2006, OCL would communicate target marketing materials and offers on behalf of its business partners in accordance with business agreements. Business partners would prepare marketing materials and specify the selection criteria for target customers. After review and approval of the marketing materials and offers,

OCL would extract the target eDM list according to requirements set by business partners. eDM would be sent out to target customers by the OCL on behalf of the business partners. The target eDM list would not be passed to the business partners throughout the process.

7.3.2 Customer Fulfilment

AAVS are processed through credit cards or bank accounts. OCL would verify and reconcile the customer information, including customer personal data of the new applicants, with the banks before an application is processed.

On some occasions, OCL would jointly run campaigns with the banks, for example, holding promotions with banks to encourage the banks' customers to join AAVS. In order to evaluate the effectiveness of such campaigns, as part of the fulfilment process, OCL would provide the list of AAVS applicants to the banks during the promotion period, including customer personal data such as:

- Full Octopus ID
- Full HKID/passport number
- Credit card number
- AAVS set-up date
- 1st AAVS reload date

The banks had already collected the above data when the customer applied for AAVS. Therefore, other than the AAVS Set-up date and 1st AAVS reload date, the banks had retained the above information prior to fulfilment of the campaigns.

7.3.3 Filtered Customer Data Shared with Business Partners

For this type of marketing activity, business partners would provide customer selection criteria to OCL. Selection criteria may include information used for filtering or screening, such as travel and spending patterns, which is stored in the cardholder database. Personal data of customers within the targeted selection criteria would be extracted from the database, and shared with the business partners for purposes such as direct mailing, telemarketing and surveying. The customers would be contacted directly by the business partners, who would then pay OCL for each successful subsequent sale. The personal data of customers for which the business partners were not able to achieve a sale case would be purged according to the operating procedures agreed between OCL and the business partners.

By inspecting OCL internal records, we identified that OCL's Octopus cardholders' personal data was shared with the following third parties:

Personal Data Recipient	Period of Sharing
AIA/AIU	July 2002 - September 2002
CIGNA	September 2002 – December 2002 (Pilot Outsourced Telemarketing Program) January 2003 – December 2005 (Outsourced Telemarketing Program and "Rewards on the Go")
CPP	September 2004 - June 2006

Besides, OCL's Octopus cardholders' personal data was shared with OCT:

Personal Data Recipient	Period of Sharing
OCT	November 2005 - February 2009

ORL used OCL's customer database for analysing customer behaviour and filtering customer records:

Personal Data Recipient	Period of Sharing
ORL	May 2008 - July 2010

Please refer to Appendix I for details of Octopus cardholders' personal data shared.

Subsequent to the corporate restructuring, OCT and ORL also shared filtered customer personal data with the following business partners and merchants for direct marketing purpose:

Personal Data Shared by	Personal Data Recipient	Period of Sharing
OCT	CIGNA	January 2006 - February 2009
	CPP	September 2006 - February 2008
	Cimigo	August 2006 - February 2008
ORL	MI	July 2007 - September 2007
	TNS	May 2008 - December 2008
	CIGNA	March 2009 - July 2010
	CPP	June 2010 - July 2010

7.4 OCL's Corporate Governance and Internal Controls

7.4.1 Audit Committee

AC was established in November 2000. It consisted of the Chairman (INED) and other two (2) NEDs. Finance Director, Head of IAD, Head of RMD and external auditor would attend the AC meetings. AC was accountable to the Board and assisted it with the monitoring of compliance with OCL's internal policies and statutory regulations. AC met three (3) times per annum to review the interim and final financial statements as well as approving the internal audit work plan which was to be executed by IAD in the subsequent year.

As part of the Audit Work Plan managed by the AC of the Board, internal audits were from time to time conducted, covering regulatory requirements, such as PDPO and the Code of Banking Practice.

7.4.2 Risk Management Committee

Since 2003, SDR assumed a risk management advisory role. RMC was established in December 2007 and consisted of the CEO and two (2) Directors (one (1) INED and one (1) NED) of the Board. RMC was accountable to the Board and assisted it with meeting its responsibilities for understanding enterprise risks (excluding Treasury) and ensuring that these risks were properly managed. RMC met three (3) times per annum to review the most significant enterprise level risks identified, the adequacy of the risk management system and the extent of its overall effectiveness.

A dedicated RMD was established in April 2008. Its role is to support the business units with managing their risks by training and supporting them in risk identification, evaluation, mitigation, monitoring and reporting. In an inquiry with the Head of RMD during the course of our fieldwork, he mentioned that RMD also considered the security and privacy requirements, including PDPO and the Guidelines, when developing and enhancing Octopus Group's internal policies and procedures.

7.4.3 Personal Data Privacy and Risk Assessments Policies

Before engaging a business partner, the business unit was responsible for performing due diligence which usually included support from RMD in conducting a risk assessment, a site visit to the potential business partner, defining data purging requirements.

In August 2005, OCL enhanced its Personal Data Protection and Privacy Policy (which was first developed in 1995) which provided guidance on handling personal data by OCL's employees, contractors and consultants.

Octopus Group also enhanced the Risk Assessment and Approval Policy in 2008 to formalise its risk assessment methodology. Risk assessments were conducted to identify, assess, mitigate and approve risks associated with new or amended business initiatives and projects.

7.4.4 Onsite Visit to Business Partners

SDR/RMD performed onsite compliance checks of the business partners and merchants, as follows:

Business Partner	Number of Visits*	With Onsite Visit Report	Without Onsite Visit Report
CIGNA	7	11/12/2006 28/06/2007 17/01/2008 25/03/2009 02/07/2010	21/06/2002 26/01/2006
Mega King Consultants Limited (outsourced telemarketer of CPP)	1	24/04/2006	N/A
Teledirect Hong Kong Limited (outsourced telemarketer of CPP)	5	02/08/2006 12/07/2010	30/08/2004 13/09/2004 28/07/2005
MI	1	01/06/2007 29/06/2007	N/A
TNS	1	N/A	24/10/2008
Cimigo	1	N/A	27/09/2007

*Includes visits with evidence of onsite visit but no Onsite Visit Report

"Onsite Visit Report" would be documented by SDR/RMD upon completion of the site visit. Such reports included an overview of the assessment and findings in the following areas:

- Physical access control;
- Servers/database security;
- Network security;
- Remote access control;
- Development system and control;
- Backup and recovery;
- Maintenance and support; and
- Other areas.

All findings and recommendations were communicated to the business partners and merchants from whom management responses were then also obtained. Follow-up of the partners' and merchants' remediation in response to recommendations made by SDR/RMD was performed in subsequent onsite visits.

7.4.5 Data Extraction Process

In January 2006, Octopus Group enhanced its data extraction architecture and process and the Planning Team of SAM was required to fill in a manual Customer Data Extraction Form (the "Form"). The Form includes details of the extraction, in particular, a short description of data to be extracted, the number of records to be extracted and the recipient of the data.

The Form was passed to senior management including Project Manager of SAM Planning Team, OCL-SAM Director or ORL Managing Director, OCT Managing Director and Head of RMD for approval. The approved Form was submitted to the Senior Manager of Infrastructure System Support Team, who then verified the approvals and passed the encrypted (PGP) extracted data to external media or relevant internal parties.

7.4.6 Data Destruction and Monitoring Process

Octopus Group further enhanced the Personal & Customer Data Protection and Privacy Policy and Procedures in 2008 and the Information Classification and Handling Guideline in 2009 to formalise the destruction process for customer personal data after the expiry of the data retention period. Octopus Group also developed a workflow document, "Record Retention Period for Personal Data", to specify the retention period for hard-copy documents, soft-copy documents and electronic records that involve customer personal data.

The physical copies of documents that were required to be kept permanently were stored by Santa Fe, the document storage vendor. Hard-copy documents reaching the expiry of their data retention period were shredded by CMDS, the paper destruction vendor, under the supervision of the management of Octopus Group.

CDs and DVDs that stored electronic personal data were shredded by the Octopus Group technical team after the expiry of their retention period. Electronic personal data records stored in application systems were destroyed after the expiry of their retention period by utilising special batch programs.

7.5 Activities Performed by OCL in Complying with PDPO and the Guidelines

7.5.1 Legal Due Diligence Procedures Performed by OCL

During our inquiries with OCL's in-house legal counsel during the course of our fieldwork, we were informed that both internal and external legal advice was obtained by Octopus Group regarding compliance with all applicable laws and regulations, including the PDPO, before the launch of the CRM pilot program with AIA/AIU in July 2002. In particular:

- OCL's in-house legal counsel commented on data ownership, personal data privacy and other issues from a legal and compliance perspective in relation to the CRM initiative;
- OCL's in-house legal counsel made recommendations regarding the control measures to be taken by OCL to outsource telemarketing activity to AIA/AIU:
    - Clear definition on the roles and responsibilities for each group of telemarketers in AIA/AIU should be documented in the agreement with AIA/AIU. An indemnity clause should also be used to protect OCL from any misconduct of AIA/AIU telemarketers;
    - The telemarketing script should be carefully reviewed and endorsed by OCL and external lawyers;
    - OCL should conduct call monitoring during the telemarketing process and all telemarketing activities should be recorded; and
    - Public relationship scripts should be prepared for possible questions from the public.
- With reference to the recommendations made by the in-house legal counsel, OCL engaged an external legal counsel to (as evidenced by a detailed fee note) review and revise the Distribution Agreement, Telemarketing Calling script and various ancillary documents, as well as to advise on OCL's role in the venture, legal structure, commercial aspects and contract negotiation. Copies of legal counsel's advice and proposed revisions were not available to us.

Our attention was drawn to a paper dated 5 July 2002 in which the Board was informed by the management that legal advice was taken to ensure the program was compliant with PDPO.

Subsequent to the pilot program with AIA/AIU, in-house legal counsel was responsible for reviewing the terms and conditions prior to entering into an agreement with business partners and no further involvement from external legal counsel was noted. As a general practice, before entering into an agreement with a business partner, terms would be negotiated and agreed with the business partners and, in some cases, documented on a term sheet and/or presented to the Senior Management Group. The agreement with the business partner would be drafted and/or

reviewed by the in-house legal team. An "Approval Form - Non-Standard Commercial Agreement/Agreement Prepared by External Parties" ("Legal Approval Form"), which was introduced in November 2003, would be used to evidence the internal approval process. The Legal Approval Form would be prepared and authorised by the SAM Director, signed off by the Legal Advisor and the Finance Director respectively. Two copies of the agreement would be sent to the business partners for signing, following which the business partner would return the original signed agreement to OCL. Once the original agreement had been returned, a copy would be filed in each of the SAM and Legal Departments. The original agreement would be kept by the Finance Director.

7.5.2 Relevant Communications with HKMA

As an Authorised Institution regulated by HKMA, OCL sent a letter to HKMA regarding the business initiative with AIA/AIU in July 2002. HKMA reminded OCL of the need to observe the customer data privacy requirements.

In January 2003, OCL wrote to HKMA regarding its intention to register as an insurance agent for direct marketing. HKMA replied in January and in March 2003 that it was inappropriate for OCL to take on the risks arising from the direct sale of insurance products and OCL should focus on payment service-related activities. HKMA considered that the risks arising from the proposed direct sale of insurance products should be properly managed and should not affect OCL's payment operations.

OCL acknowledged the view of HKMA and decided that OCL would implement a corporate restructuring process. The non-payment service-related activities would be carried out by separate legal entities. OCL suspended the marketing activities with CIGNA on selling insurance products and other CRM activities from August 2003.

7.5.3 Relevant Communications with PCPD

Since 2004, PCPD received several complaints from the public regarding Octopus Group, in respect of the use of personal data for direct marketing purposes.

PCPD received a complaint case on a lucky draw program jointly conducted by OCL and an insurance company, and sent a letter to OCL in February 2004 inquiring about the collection of HKID information for use in lucky draws as well as the provision of free insurance products. Subsequent to further communication between OCL and PCPD, OCL updated the terms and conditions and then ceased maintaining full HKID numbers for lucky draw purposes. PCPD replied in May 2004 that they had decided not to proceed with further investigation.

In May 2007, PCPD issued a letter to OHL regarding a complaint on and inquiry of the security measures taken by Octopus Group to protect personal data in relation to the sharing of personal data with OCT under the Octopus Rewards Program, as well as the secondment arrangement for marketers of a life insurance company. Subsequent to the further communications between OHL and PCPD, ORL and the insurance company entered into a contractual agreement in March 2009 as an Octopus Rewards Program partner. PCPD replied in the same month that they had decided not to proceed with further investigation.

OCL took corresponding actions in accordance with PCPD's guidelines and regulations to address PCPD's concerns. Please refer to Appendix II for details.

PCPD issued an interim report on 30 July 2010 with the objectives of keeping the public informed of the progress of the investigation, and providing timely suggestions to ORL on related good practices. The areas covered in the interim report include:

- Collection of personal data;
- Personal data necessary for enjoying the basic benefits;
- Bundled consent;
- Use of personal data; and
- Further disposals of the data by third parties.

PCPD then completed its investigation of ORL regarding the personal data collected and disclosed under the Octopus Rewards Program. PCPD's final report of this investigation was published on 18 October 2010.

7.6 Recommendations

Our recommendations set out below are only those that came to our attention during the course of our work and relate to the practices and processes of OCL prior to the cessation of sharing of personal data with third parties in July 2010. They are summarised in the following areas:

- Corporate and data governance structure;
- Policies and procedures;
- Due diligence and controls to govern the disclosure of personal data to third parties;
- Collection of personal data; and
- Data storage and retention.

PCPD is the statutory body on personal data privacy protection matters and our recommendations have taken into account the comments made by PCPD in his interim report on ORL. PCPD has subsequently completed the investigation of ORL and issued its final report for this investigation. PCPD has also published a revised guideline on direct marketing to help data users comply with its guidelines and regulations when using personal data for direct marketing activities. OCL should observe and comply with PCPD's revised guidelines, as well as the recommendations in the final report for PCPD's investigation for any use of personal data in the future.

7.6.1 Corporate and Data Governance Structure

OCL established an AC and RMC to serve as risk management and compliance monitoring functions. Furthermore, an enterprise risk management framework was established to facilitate the management of enterprise risks.

However, in view of increasing public concerns and customer expectations, OCL may consider taking a more proactive approach to address privacy and personal data protection by strengthening its corporate and data governance structure.

To ensure sufficient Board and senior management oversight on data privacy, OCL may consider improving its existing corporate and data governance structure for data privacy by either expanding the terms of reference of existing RMC or establishing a specific Data Privacy Committee, as well as strengthening the role of AC and IAD.

Since 2005, the Managing Director of OCT assumed the role of the Data Protection Officer for Octopus Group until Head of SDR took up the role in July 2007. When the Head of RMD reported for duty in May 2008, he assumed the role of the Data Protection Officer of Octopus Group. However, the roles and responsibilities for personal data privacy protection were not clearly defined. A designated privacy officer with relevant experience should be formally appointed whose main responsibility is to manage OCL's overall privacy and personal data protection and take responsibility for OCL's personal data governance, privacy compliance and scrutiny of any personal data protection-related matters.

While risk assessment including customer data protection is conducted according to Risk Assessment and Approval Policy for new and change initiatives, OCL may consider conducting PIA and PCA to ensure privacy risks in existing business processes and new business initiatives or projects are carefully considered, identified and managed.

Privacy awareness training programs could be further enriched to promote a culture of information security and privacy awareness.

7.6.2 Policies and Procedures

OCL developed and adopted a number of information security and privacy policies, procedures and guidelines. RMD considered the security and privacy requirements, including PDPO and the Guidelines, when developing and enhancing the internal policies and procedures. OCL may consider enhancing the existing policies and procedures by developing an integrated and consistent information security and privacy policy framework that is structured, simplified and accessible to its staff. The new framework should form the basis of all information security and privacy policies, procedures, guidelines and awareness training programmes. Existing information security and privacy procedures and guidelines should also be enhanced and regularly communicated to staff, including the detail requirements of PDPO, the Code of Practice and other relevant Guidelines issued by PCPD and other regulatory authorities.

While OCL has defined the Asset Ownership under Security Responsibility and Incident Reporting Policy and information classification into highly sensitive, confidential, internal and unclassified, controls and accountability for information assets should be clearly defined in the policies and procedures. OCL may consider classifying information assets in terms of their confidentiality, sensitivity, legal and reputational risk and to ensure that all assets are accounted for and have a nominated information asset owner (who should be senior management personnel, if appropriate) responsible for overseeing their privacy and personal data protection.

OCL may also consider enhancing its procedures for handling the DAR and DCR made by customers. Detailed procedures for the DAR and DCR should be clearly defined in order to fulfil the requirement in the PDPO.

7.6.3 Due Diligence and Controls to Govern the Disclosure of Personal Data to Third Parties

Octopus Group ceased the sharing of personal data with third parties in July 2010. If Octopus Group carries out similar business activities in the future, with regard to the controls to govern the disclosure of personal data, contractual arrangements should be made with business partners to ensure that customers are being notified of the true identity of the telemarketer and which insurer they represent. Third party compliance monitoring should also be enhanced in respect of each business partner and outsourced call centres to ensure that proper controls have been put in place and are operating effectively.

Legal due diligence process was carried out by OCL's internal/external legal counsel for the compliance of the relevant laws and regulations, including PDPO. Enterprise risks relating to the disclosure of personal data have been identified and mitigating controls have been established prior to engaging in business contracts. OCL also took corresponding actions in accordance with PCPD's guidelines and regulations to address PCPD's concerns regarding the complaint cases. However, the existing due diligence process can be further enhanced. Currently, SAM would request the Legal Department to review the agreement only when it was for new business initiatives with identifiable risks to the Octopus Group. Since the increasing complexity of the business arrangement would give rise to the legal risks, except for the business arrangements under pre-approved standard agreements, all agreements should be reviewed by the Legal Department to ensure that all relevant regulatory requirements are properly addressed.

Octopus Group developed a workflow document, "Record Retention Period for Personal Data", to specify the retention period for hard-copy documents, soft-copy documents and electronic records that involve customer personal data. However, OCL may consider to strengthen the record retention process relating to legal due diligence performed, the customer data extraction, data purging and destruction conducted by third parties, and monitoring of compliance with the confidentiality and personal data protection measures performed by the personal data recipients should be properly retained as audit trail.

With reference to the suggestions on related good practices stated in the interim report issued by PCPD and the principles laid down by the recent Administrative Appeals Board decision in August 2010, if Octopus Group carries out similar business activities in the future, only limited customer personal data should be passed to third parties in order to reduce the privacy risks associated with its sharing and use. The tracing of data extraction and sharing should be automated to ensure the validity of data provided to third parties and to detect irregularities and cases of non-compliance with the PDPO more easily.

7.6.4 Collection of Personal Data

The customer was not required to provide personal data for the usage of A-card. OCL only collected customers' personal data via various registration and application forms for issuance of P-card and AAVS. The primary purposes of collecting the personal data were to provide lost card reporting services and processing of automatic reloading for payment through Octopus card, as well as complying with the "know-your-customer" principle under the Guideline on Prevention of Money Laundering issued by HKMA.

As stipulated in the Terms of Application for Personalised Octopus, applicants to the program agreed that such personal information can be used by OCL and its subsidiaries/affiliates/business partners for marketing purposes. The Octopus cardholders can opt out of receiving direct marketing materials by calling a hotline, visiting website or in writing.

Taking into account the latest suggestions on related good practices stated in the interim report issued by PCPD, as well as the principles laid down by the recent Administrative Appeals Board decision in August 2010, OCL may consider improving its existing processes for the collection of customers' personal data, and the manner of the personal data collection should be enhanced, including:

- Collection of personal data;
- Personal data necessary for enjoying the basic benefits;
- Font size of the application form;
- Bundled consent;
- Use of personal data;
- The purpose and the class of transferee that will use the data;
- Options for customer to elect not to receive any direct marketing materials; and
- Further disposals of the data by third parties;

PCPD published a revised Guideline on the Collection and Use of Personal Data in Direct Marketing in October 2010 to help data users comply with its guidelines and regulations when using personal data for direct marketing activities. OCL should observe and comply with PCPD's revised guidelines, as well as the recommendations in the final report for PCPD's investigation for any use of personal data in the future.

7.6.5 Data Storage and Retention

OCL and ORL collected and stored customer personal data in separate systems. Customer personal data and transaction records from OCL and ORL systems are duplicated to the CRM System daily for data analysis. The CRM System was shared amongst OCL, OCT and ORL. Although personal data collected by OCL and ORL were stored in different tables within the CRM System, only authorised users of SAM could access both tables and no audit trails were available to ascertain which tables were being accessed to extract the customer personal data.

OCL had developed an information system to support daily business operations such as a customer service hotline. Security measures were implemented and users were not allowed to perform wildcard inquiries of customer records. However, sensitive personal data, including HKID number, should be masked during on-screen inquiry of batch or customer summaries in order to reduce the risk of data leakage.

Customer personal data should also be purged when the personal data is no longer required. To comply with the established personal data retention period practice, the existing personal data retention and destruction policies may be enhanced to cover all types and formats of customer personal data and to ensure that data records are stored no longer than necessary.

End

Appendix I
Summary of Octopus Cardholders' Personal Data Shared with Third Parties

Please refer to below table for details of OCL's Octopus cardholders' personal data shared with third parties. This summary was prepared based on the documentation and records available to us during the course of our fieldwork:

Personal Data Shared by	Personal Data Recipient	Period of Sharing	Estimated Number of Records Shared	Data Fields Shared	Purpose of Sharing
OCL	AIA/AIU	July 2002 – September 2002	35,000	English name Chinese name HKID number Date of birth Home phone Office phone Mobile phone Mailing address	To conduct a trial co-operative marketing program with AIA/AIU to cross-sell its personal accident insurance plans by making telemarketing calls to the selected customer list
OCL	CIGNA	September 2002 – December 2002 (Pilot Outsourced Telemarketing Program) January 2003 – December 2005 (Outsourced Telemarketing Program and "Rewards on the Go")	320,000	Customer name Home phone Office phone Mobile phone HKID number Date of birth Address Bank/credit card number	To conduct a pilot for an outsourced telemarketing program between OCL and CIGNA to cross-sell CIGNA's insurance products To provide free insurance plans to participants of the "Rewards on the Go" lucky draw program and cross-sell CIGNA's insurance products

Personal Data Shared by	Personal Data Recipient	Period of Sharing	Estimated Number of Records Shared	Data Fields Shared	Purpose of Sharing
OCL	CPP	September 2004 – June 2006	300,000	Customer name Customer Chinese name Home phone Office phone Mobile phone Octopus ID (partial) HKID number Date of birth (partial Mailing address AAVS credit card number	To conduct a co-operative marketing program between OCL and CPP to cross-sell CPP's card protection insurance plans by making marketing calls to the selected customer list AAVS credit card number was shared with CPP for premium payment upon customer consent

Please refer to below table for details of OCL's Octopus cardholders' personal data shared with OCT:

Personal Data Shared by	Personal Data Recipient	Period of Sharing	Estimated Number of Records Shared	Data Fields Shared	Purpose of Sharing
OCL	OCT	November 2005 – February 2009	All records in OCL's customer database	All data fields in OCL's customer database	To assign the right to use OCL's customer database by OCT in relation to the sharing of selected customer list with OCT's business partners for conducting marketing and research activities

Please refer to below table for details of ORL used OCL's customer database for analysing customer behaviour and filtering customer records:

Personal Data Shared by	Personal Data Recipient	Period of Sharing	Estimated Number of Records Shared	Data Fields Shared	Purpose of Sharing
OCL	ORL	May 2008 – July 2010	All records in OCL's customer database	All data fields in OCL's customer database	To assign the right to use OCL's customer database by ORL in relation to the analysis of customer behaviour and filtering of customer records

Appendix II
Prior Communications with Privacy Commissioner of Personal Data

PCPD has received some complaint cases from the public in relation to Octopus Group. There are in total fifteen (15) compliant cases as at the date of this Report. Please refer to below table for details:

	Period	Entities	Description of Complaints	Actions by Office of Privacy Commissioner	Actions by Octopus Group	Status
1.	February 2004 – May 2004	OCL	Collection of HKID for a lucky draw program and provision of free insurance by an insurance company	• Requested information on a lucky draw program • Requested OCL to revise Terms of Application of the lucky draw program • Requested OCL to stop collecting dates of birth of ineligible participants of free insurance plan • Requested OCL to immediately delete the dates of birth of ineligible participants of free insurance plan	• Incorporated the "Notes" section into the Terms of Application of the lucky draw program in accordance with PCPD's recommendation • Considered it was necessary to collect the dates of birth of all participants • Stopped keeping the full HKID number for lucky draw purpose	PCPD issued a letter of no further action in May 2004
2.	February 2004 – March 2004	OCL	Use of personal data of the participants in a lucky draw for sale of insurance products	• Inquired OCL of the response to the complaint case • Inquired OCL of whether the complainant's full HKID	• Set out the reasons for the collection of personal data from the successful participants in the lucky draw and the	OCL replied to PCPD in March 2004. No further correspondence was noted

	Period	Entities	Description of Complaints	Actions by Office of Privacy Commissioner	Actions by Octopus Group	Status
				number was still being retained	subsequent use of the data • Stopped retaining the full HKID number of the participants for the purpose of lucky draw	
3.	January 2005 – February 2005	OCL	Collection of personal data of participants for lucky draw and use for provision of insurance policy by an insurance company	• Inquired on a lucky draw program • Expressed the view that participants would not be aware that one of the purposes of collecting their personal data was the provision of the insurance product • Expressed the view that for offering birthday promotion, the collection of month and year of birth should suffice • Inquired OCL of the response to PCPD's comments	• Put the collection purpose in a conspicuous and prominent manner • Considered alternative ways for collection of age-related information • Continued to adhere to all requirements of DPP	PCPD issued a letter of no further action in February 2005
4.	May 2005 – June 2005	OCL	Receipt of marketing mails after the customer alleged that he made an email request for an opt-out	• Inquired OCL of the response to the complaint	• Explained that the complainant's email request might have been lost during transmission • Removed the relevant customer from the distribution list	PCPD issued a letter of no further action in June 2005

	Period	Entities	Description of Complaints	Actions by Office of Privacy Commissioner	Actions by Octopus Group	Status
5.	August 2007 – January 2008	OCL OHL	Collection of HKID number for application of property resident card	• Requested information and clarifications on collection of personal data in application of property resident card •	• Explained the purpose of information collected for application of property resident card • Mentioned that the property management office no longer handled the application of personalised Octopus Cards	OCL replied to PCPD in January 2008. No further correspondence was noted
6.	December 2005 – January 2006	ORL	Provision of complainant's personal data contained in the application form of Octopus Rewards Program to an outsourced company	• Requested ORL to confirm whether the complainant's application form was collected • Requested information on the transfer of the complainant's personal data to an outsourced company	• Provided the complainant's application form per PCPD's request • Mentioned that the complainant consented to the terms and conditions that his personal data would be used for the purpose of member registration • Explained that the complainant's personal data was thus disclosed to OCT	PCPD issued a letter of no further action in January 2006
7.	July 2006 – November 2006	OHL	Transfer of personal data to an insurance company's telemarketing staff for sale of insurance plan without the complainant's consent	• Requested information on the transfer of the complainant's personal data to the insurance company • Requested details of the insurance product and the cooperation agreement between OCT and the insurance company	• Provided voice recording tapes and signed registration form to PCPD • Clarified that the telemarketing officer was an employee of the insurance company who was appointed under an outsourcing agreement with OCT in making marketing calls	OHL replied to PCPD in November 2006. No further correspondence was noted

	Period	Entities	Description of Complaints	Actions by Office of Privacy Commissioner	Actions by Octopus Group	Status
8.	May 2007 – March 2009	OHL	Concerns over secondment of an insurance company's telemarketers and transfer of personal data to the insurance company, and security measures taken to protect the personal data in relation to the transfer	• Requested details on the extent which the staff of the insurance company as telemarketers is allowed to access the OCT database • Inquired OHL of the security measures taken to protect personal data	• Described the cooperation with the insurance company and purposes of transferring the personal data to telemarketers • Explained the restriction of telemarketers to access the OCT database • Mentioned that the Octopus Reward scheme was voluntary and its members could opt out of receiving direct marketing materials at any time	PCPD issued letter of no further action in March 2009
9.	May 2007 – December 2008	OCL OHL	Concerns over collection of HKID number for AAVS	• Requested OCL to take steps to desist from the practice of collecting HKID number from anonymous Octopus cardholders applying for AAVS	• Amended the AAVS terms and conditions to remind existing anonymous Octopus cardholders with AAVS that their identities had been associated with HKID	PCPD issued a letter of no further action in December 2008
10.	July 2007 – September 2007	OHL	Unauthorised disclosure of Personalised card transaction records	• Requested OHL to confirm the collection purposes of the complainant's personal data • Requested OHL to confirm and state the purposes of disclosing the complainant's personal data	• Implemented exceptional procedures to block the disclosure of transaction records • Agreed with the complainant to maintain the telephone reporting lost card function • Designated specific staff to handle the complainant's further enquiries	PCPD issued a letter of no further action in September 2007

	Period	Entities	Description of Complaints	Actions by Office of Privacy Commissioner	Actions by Octopus Group	Status
11.	May 2010 – June 2010	OCL	Collection of personal data for refund of A-card	• Referred to letter of complaint in April 2010 • Requested for information regarding Octopus card refund process	• Explained that the purpose of collecting personal data such as name and contact number was for OCL to follow up inquiries and the refund process	PCPD issued a letter of considering the case in June 2010. No further correspondence was noted
12.	May 2010	OCL	Collection of personal data for refund of A-card	• During the course of our fieldwork, OCL was still in communication with PCPD	• During the course of our fieldwork, OCL was still in communication with PCPD	During the course of our fieldwork, OCL was still in communication with PCPD
13.	May 2010	OCL	PCPD Inquiry over use of personal data in commercial and transit applications of Octopus cards	• Inquired on commercial and transit applications of Octopus cards • Requested further information on security measures taken by OCL to protect personal data from unauthorised or accidental access and the selling of personal data for profits.	• Provided responses and information and as requested by PCPD	OCL replied to PCPD in May 2010. No further correspondence was noted
14.	August 2010	OHL	Investigations of the use of personal data by Octopus Group with its cooperation with business partners following public concern	• Inquired on OHL's press release dated 13/08/2010 • Requested information regarding the investigation	• Provided responses and information as requested by PCPD	Final investigation report was published by PCPD on 18 October 2010

	Period	Entities	Description of Complaints	Actions by Office of Privacy Commissioner	Actions by Octopus Group	Status
15.	July 2010	OHL	PCPD inquiry on the use of personal data of the Octopus Rewards Program members for conducting marketing surveys for a marketing survey company	• Inquired on conducting marketing surveys for a marketing survey company	• Provided information as requested by PCPD	During the course of our fieldwork, OHL was still in communication with PCPD

Deloitte
德勤

Octopus Cards Limited

Addendum to the Final Report on the Independent Assessment and a [illegible] Hong Kong Holdings Limited Detailed Findings and Recommendations

26 November 2010

Enterprise Risk Services

Contents

Acronyms

AC	Audit Committee
AAVS	Automatic Add Value Service
Board	Board of Directors
CEO	Chief Executive Officer
CIGNA	CIGNA Worldwide Insurance Company
Cimigo	Cimigo Limited
CPP	Card Protection Plan Limited
CRM	Customer Relationship Management
DAR	Data Access Request
DCR	Data Correction Request
DPP	Data Protection Principles
HKID	Hong Kong Identity Card
HKMA	Hong Kong Monetary Authority
IAD	Internal Audit Department
INED	Independent Non-executive Director
MI	Magazine International (Asia) Limited
NED	Non-executive Director
OCHS	Octopus Clearing House System
OCL	Octopus Cards Limited
OCT	Octopus Connect Limited
Octopus Group	Octopus Holdings Limited and its subsidiaries
ORL	Octopus Rewards Limited
PCA	Privacy Compliance Assessment
PCPD	Office of Privacy Commissioner of Personal Data
PDPO	Personal Data (Privacy) Ordinance
PIA	Privacy Impact Assessment
RMC	Risk Management Committee
RMD	Risk Management Department
SAM	Sales and Marketing Department
SDR	Strategy, Development and Risk Management Department
TNS	Taylor Nelson Sofres Hong Kong Limited
T&C	Terms and Conditions

Important Notes to Reader

This Addendum is solely prepared for the purpose set forth in Section 1 of the Final Report on the Independent Assessment under Section 59(2) of the Hong Kong Banking Ordinance (the "Final Report") and for OCL information, and is not to be used for any other purposes. The Addendum and the Final Report are collectively referred to as the "Report". Our Report will not include any representation as to the quality or performance of the OCL's goods or services nor their fitness or suitability for any customer's intended purpose.

In preparing our Report, we have relied upon the representations made to us by the management, officers and staff of OCL and on the materials made available to us for the purposes of the Assessment. OCL's management warrants that the information provided and materials made available to us are correct to the best of their knowledge and belief and that there will be no other information the omission of which may cause us to be misled or which may appear to be misleading.

Our work does not entail us performing detailed tests of transactions to the extent that would be necessary to disclose all defalcations and irregularities which may exist. Accordingly, reliance should not be placed on our Report to disclose all such matters.

The matters raised in this Report are only those that came to our attention during the course of our field visit. They are not necessarily a comprehensive statement of all the weaknesses that may exist relating to OCL or all the improvements that could be made. The recommendations for improvement that we make should be assessed by OCL for their full commercial and cost implications before they are implemented.

This Report does not constitute either an audit or review in accordance with the Hong Kong Institute of Certified Public Accountants or with any other auditing standards and, consequently, no such assurance is expressed. Your attention is drawn to Section 5 of the Report for the limitations of our Assessment.

We do not assume responsibility towards or accept liability to any other person for the contents of this Report. For the avoidance of doubt, all duties and liabilities (including without limitation, those arising from negligence) to any third party (being any party who is not a contractual party to the engagement letter pursuant to which this Report is issued) is specifically disclaimed.

Except for internal use or otherwise mentioned above, if OCL intends to publish or reproduce our Report or any part thereof in any document (including electronic formats or other media), or otherwise make reference to DTT/HK in a document (including electronic formats or other media) that contains other information, OCL agrees that prior to making any such use of our Report, or reference to DTT/HK, to (1) provide us with a draft of the document to read and (2) obtain our approval for the inclusion or incorporation by reference of our Report, or the reference to DTT/HK, in such document before the document is published and distributed.

Detailed Findings and Recommendations

Our findings and recommendations set out below are only those that came to our attention during the course of our work and relate to the practices and processes of OCL prior to the cessation of sharing of personal data with third parties in July 2010. They are summarised in the following areas:

- Corporate and data governance structure;
- Policies and procedures;
- Due diligence and controls to govern the disclosure of personal data to third parties;
- Collection of personal data; and
- Data storage and retention.

PCPD is the statutory body for personal data privacy protection matters and our recommendations have taken into account the comments made by PCPD in its interim report on ORL. PCPD has subsequently completed its investigation of ORL and issued its final report for the investigation. PCPD has also published a revised guideline on direct marketing to help data users comply with its guidelines and regulations when using personal data for direct marketing activities. OCL should observe and comply with PCPD's revised guideline, as well as the recommendations contained in PCPD's final report for its investigation, for any use of personal data in the future.

Corporate Governance and Data Governance Structure

1. **Corporate governance should be strengthened by improving the risk management and compliance monitoring on data privacy.**

   OCL established its AC and RMC in 2000 and 2007 respectively for serving as its audit, risk management and compliance monitoring functions. A risk management framework was established in 2008 to facilitate the effective management of enterprise risks. According to the "Risk Management Policy & Framework", there were three lines of risk management function:

   - Business units - responsible for effective management of risks in first line operations and business process level;
   - RMC and RMD - responsible for risk management to ensure the business units manage the risk and controls effectively; and
   - AC and IAD - responsible for internal audit function to assure the first two lines of operations against the risk profile of OCL.

   Currently, AC consists of the Chairman (INED) and other two (2) NEDs. Finance Director, Technical Director, Head of IAD, Head of RMD and the external auditor would attend the AC meetings. Meanwhile, RMC consists of the CEO and two (2) Directors (one (1) INED and one (1) NED) of the Board. Finance Director, Technical Director, Head of Operations, In-house Legal Counsel and Head of RMD would attend the RMC meetings. Both AC and RMC meet three times a year to assume their risk management and compliance monitoring functions.

   In view of increasing public concern and to ensure sufficient board and senior management oversight regarding data privacy, the corporate governance should be strengthened by improving the risk management and compliance monitoring on data privacy. The following areas of concern relating to personal data privacy should be addressed accordingly:

   - Oversight of OCL's privacy and data protection methodology;
   - Monitoring of the impacts of changes in legal and regulatory requirements relating to privacy of personal data;
   - Evaluation of existing data protection measures;
   - Periodic review of privacy policies and procedures; and
   - Promotion of a culture of privacy and security awareness throughout the organization.

   For example, the terms of reference of the AC and RMC should be expanded to include the oversight of data privacy. Regular monitoring, discussion and evaluation of the effectiveness of managing data privacy risk should be carried out.

   Alternatively, OCL should consider establishing a Data Privacy Committee to oversee privacy-related issues generated by its business to enhance the leadership and governance of data privacy and data security. Any major business initiatives and their associated privacy risks should be discussed in the Data Privacy Committee and reported to the Board.

The AC serves as the Board's "eyes and ears" in monitoring compliance with OCL's policies and other internal and statutory regulations. In addition to its existing responsibilities, the AC should take a more proactive approach to understand the privacy risks generated by the business units. The AC should provide an oversight and independent view to the major business decisions of the Board, and to ensure appropriate action is taken to deal with privacy risks or other control weaknesses.

2. **The compliance function should be strengthened and a designated privacy officer should be appointed to manage overall privacy and personal data protection matters.**

Currently, the compliance functions are shared by different departments. The responsibility of regulatory compliance was taken by Finance Director from the establishment of OCL. Following the establishment of OCT in 2005, the Managing Director of OCT took up the role of Data Protection Officer until Head of SDR took up the role in July 2007. When Head of RMD reported duty in May 2008, he assumes the role of Data Protection Officer of OCL.

However, the roles and responsibilities of personal data privacy protection were not clearly defined in the job description. A designated privacy officer with relevant experience should be formally appointed whose main responsibility is to manage the overall privacy and personal data protection matters for OCL. The responsibilities of the privacy officer should include, but not limited to the following areas and should be clearly documented as terms of reference.

- Ensuring the overall personal data governance and the compliance of PDPO and Code of Practice/guidelines published by PCPD;
- Developing and enhancing all privacy and data protection policy, procedures and guidance;
- Conducting training to the employees and ensuring that they observe and comply to OCL's privacy policy;
- Producing regular reports on privacy compliance;
- Monitoring changes to systems and documentation to ensure compliance with PDPO and Code of Practice/guidelines published by PCPD;
- Ensuring that retained personal data is secured and not retained for any time longer than necessary for the purpose it was acquired for;
- Complying to data access request and data correction request under PDPO, Code of Practice and guidelines published by PCPD as well as the established policy, procedures and guidelines;
- Working closely with PCPD and other public authorities for any investigation of privacy related complaints; and
- Handling general issues concerning privacy and personal data protection.

3. **PIA/PCA should be conducted to ensure the privacy risks of the existing business processes and new business initiatives or projects have been carefully considered, identified and managed.**

OCL established the "Risk Assessment and Approval Policy" to formalise the risk assessment methodology. Risk assessments would be conducted to manage the risks associated with new or change of business initiatives and projects, such as the review of Octopus card systems security, and network security. It facilitates understanding of how the business initiatives or changes align with OCL's strategic direction and risk appetite.

For instance, taking into consideration of HKMA issued data privacy circular on 10 July 2008, OCL has conducted external security audit in 2008 to review the customer data protection measures. The scope of review was endorsed by the Board and RMC.

In view of the amount of personal data collected and processed every day by OCL, highest priority must be given to privacy and data protection during the risk assessments. OCL should conduct comprehensive PIA /PCA on existing business processes as well as the new business initiatives or projects.

PIA should be conducted for identifying and mitigating any privacy risks associated with the new business initiatives or projects, which involves collection and processing of personal data, implementation of techniques or technology that may be privacy intrusive, or change in the business process that may result in expanding the scope of personal data to be collected or processed. PIA allows OCL to adequately consider the impact on personal data privacy before project commencement, and addressing the privacy problems identified at the early stage.

PCA should also be conducted at least once a year to assess and evaluate the level of privacy compliance with the PDPO, code of practices issued by PCPD and other relevant guidelines. The scope should include

review of the existing business processes and information systems in relation to collection and processing of personal data.

Detailed reports with recommendations should be given after conducting the PIA and PCA to ensure that OCL has taken adequate measures to comply with the PDPO and other related guidelines. OCL should carefully consider the recommendations and eradicate the problems in a timely manner.

4. **Privacy awareness training program should be further developed to promote information security and privacy awareness culture.**

Currently, the information security awareness training is delivered to the staff by RMD through online e-learning module. It is hosted on OCL's intranet which contains five sections in providing guidelines on general information security measures to the staff (including "Desktop security", "Leaving your desk", "Working remotely from the office", "Verbal communication" and "Handling Information"). New staff is required to complete the online e-learning module within two months from the first working day.

In addition, Human Resources and Administration Department circulates the "Personal & Customer Data Protection and Privacy Policy" to all new staff on the first working day, and they are required to sign the employee agreements declaring that they have read, understood and will comply with the policy.

In order to strengthen the information security and privacy awareness culture, the existing information security awareness training programme should be redesigned into a more structural and privacy compliance focused training. It should cover the overall information security and privacy policy of OCL, PDPO, in particular its six DPP, and other related regulations. The content of the training should be periodically reviewed and updated to reflect the changing privacy regulations and requirements. The training should be mandatory to all staff and conducted at least once a year.

Other measures should also be considered to further enhance the overall information security and privacy awareness culture:

- Induction session for new staff that emphasise the importance of personal data privacy should be conducted;
- Use of alternative channels to maintain staff awareness on personal data privacy. For example:
  - posters about privacy awareness could be pinned up prominently on staff common areas;
  - installing computer screensavers which promote the importance of information security and data protection;
  - privacy newsletter could be circulated to update the staff about the latest privacy and security risks;
  - personal data privacy culture survey can be conducted to understand and assess the level of privacy culture;
  - creating events and slogans that will raise the attention of the staff to personal data privacy; and
- Tailored workshops should be conducted to business units which will frequently collect and/or handle the customer personal data.

Policies and Procedures

5. **The information security and privacy policies, procedures and guidelines should be further enhanced and regularly reinforced.**

OCL published a number of information security and privacy policies, procedures and guidelines. The "Security Policy Framework" consists of four sets of security documents each service different security objectives, namely:

- Master Security Document Set;
- User Security Document Set;
- IT Security Document Set; and
- Octopus Product Security Document Set.

Another set of policy and procedure in relation to privacy is also established, namely:

- Personal & Customer Data Protection and Privacy Policy; and
- Personal & Customer Data Protection and Privacy Procedure.

This established framework provides the requirements on information security and handling of personal data of OCL and its staff.

Existing privacy procedures and guidelines should be further enhanced to address the necessary component as required by PDPO, Code of Practice and other relevant Guidelines issued by PCPD and other regulatory authorities. The contents of the procedures and guidelines and how it would be applied in their daily tasks should be periodically communicated to the staff. The procedures and guidelines should also be reviewed and updated regularly.

In particular, the following areas should be strengthened in the policies, procedures and guidelines:

- Data retention policy and procedure should be enhanced to ensure that personal data is not retained any longer than necessary;
- Policy and procedure in relation to the handling of DAR and DCR from the data subject should be documented, such as handling the DAR and DCR within 40 days after receiving the request, and maintaining a log book of any refusal cases to DAR and DCR for a minimum period of four years;
- Strengthen the constant monitoring and adoption of the legal regulations and requirements changes in relation to privacy;
- Compliance monitoring plan could be further enhanced to include the requirement of PIA and PCA; and
- Formal disciplinary policy should be developed to prevent staff, contractors and third party users in violating the privacy policies and procedures.

6. Ownership of information asset and increasing the accountability of the information asset owner of personal data should be clearly defined.

OCL established the "Information and Classification Guideline" to provide the guidance for handling OCL's information asset. According to the guideline, information is classified into four categories: "Unrestricted", "Internal", "Confidential" and "Highly Sensitive". Currently, personal data of the customer is defined as "Highly Sensitive", and it should not be removed from office premises without express approval from the information asset owner.

The information asset owners are defined in the "Risk Responsibility – Incident Handling & Reporting Policy", for which consumer personal data are owned by SAM and consumer records are owned by Operations Department. However, no designated owner is clearly defined and therefore it appears to be difficult to establish the accountability of any privacy and personal data related matters.

OCL should enhance the information asset classification such that all assets are accounted for and have a designated information asset owner (who should be senior management personnel if appropriate) to oversee the privacy and personal data protection. The responsibility for the protection of information asset could be delegated by the owner as appropriate, but the information asset owner should be held accountable for the protection of the information assets, in particular, protection of personal data of the customers.

Information asset of personal data should also be granularly classified in terms of its confidentiality, sensitivity, criticality and legal requirements to OCL and its customers. The information asset owner should define and periodically review the information asset classification to ensure it is kept up to date in view of the constantly changing legal regulations and requirements in relation to privacy.

Due Diligence and Controls to Govern the Disclosure of Personal Data to Third Parties

7. Octopus Group should strengthen the due diligence process on data privacy in establishing and maintaining business arrangement with partners.

Due Diligence Reviews Prior to Engaging Business Partners

Prior to May 2008, SDR served the risk advisory function (including privacy risk) but it was not compulsory to obtain approval before engaging with Business Partners. In May 2008, Octopus Group established RMD to assess the risk of a business arrangement.

Before engaging a business partner, the RMD performed due diligence review by conducting risk assessment and site visit to the potential business partners to assess any potential risk in establishing business arrangement. However, the risk assessment mainly focused on financial, operational, contractual and reputational risks, whereas risks in usage and sharing of customer personal data to business partners may not be sufficiently addressed and documented. As passing customer personal data to third parties may have

potential adverse implication on reputation risk and legal, regulatory and contractual risk, a standardised and comprehensive risk assessment associated with personal data privacy should be further enhanced.

Legal Review of Agreements

Subsequent to a satisfactory result from the due diligence process, the SAM would preliminary assess the impact of entering into an agreement with the business partner. Whenever is needed, RMD would assist the SAM to define data purging requirements and obtain legal advice on such business arrangements in order to fulfill the regulatory requirements, such as PDPO and Code of Banking Practice. Business terms would be agreed with the business partners and in some cases, documented on a term sheet. The agreement with the business partners would then be drafted and/or reviewed by the In-house Legal Team. Based on the agreed draft of the agreement, an "Approval Form - Non-Standard Commercial Agreement/Agreement Prepared by External Parties" ("Legal Approval Form") would be prepared and circulated to the following parties for signoff/approval:

- Preparer and authoriser: SAM
- Checker: In-house Legal Counsel
- Approver: Finance Director

However, it was noted that SAM would request the In-house Legal Counsel to review the agreement only when it was for new business initiatives with identifiable risks to the OCL. Since the increasing complexity of the business arrangement would give rise to the legal risk, except for the business arrangements under pre-approved standard agreements, all agreements should be reviewed by In-house Legal Counsel to ensure the compliance with the relevant regulatory requirements, including PDPO. All contracts should be appropriately supported by the Legal Approval Form.

Maintenance of the Agreements

If the agreement was approved under the Legal Approval Form process, two sets of the agreement would be sent to the business partners for endorsement. Once the physical copy of the agreement has been returned to the SAM, the original agreement would be kept by the Finance Director and copies of the agreement would be filed in the SAM and In-house Legal Team. For those agreements which have not gone through the Legal Approval Form process, however, there was not a mandatory requirement to maintain copies of the agreement in SAM, In-house Legal Team and Finance Department altogether, nor keeping a master list to keep track of the location of the contracts.

To ensure the completeness of the contracts and enable the management to understand the legal position of OCL as a whole, a master list, together with a full set of agreements should be maintained by a designated process owner in a centralised manner.

8. **The transparency of direct marketing business arrangement to customers should be increased.**

Between 2003 – 2006, OCL had entered into an agreement with CIGNA to perform telemarketing services to customers extracted from its customer base. The actual arrangement was that Octopus Group extracted call lists and sent directly to CIGNA staff for telemarketing purpose. CIGNA staff performed telemarketing within CIGNA's office premises while representing themselves as personnel of Octopus Group. As a result, customers may have been initially unaware that the calls were made by CIGNA telemarketers instead of Octopus employees.

In a recent decision of the Administrative Appeals Board dated 19 August 2010 regarding Wing Lung Bank Limited v Privacy Commissioner for Personal Data [AAB 38-2009], it is determined that any possible misrepresentation should be avoided as to the true identity of the insurer.

Subsequent to the corporate restructuring, the CRM business was transferred out of OCL. Octopus Group also ceased the sharing of personal data with third parties in July 2010. If Octopus Group carries out similar business activities in the future, providing that customers made consent to Octopus Group in passing their personal information to business partner for direct marketing purpose, Octopus Group should request its business partner to disclose the nature of the direct marketing arrangement with Octopus Group when introducing the services to potential customers. Therefore, they are well informed of whom they were contacted by and how the arrangement was made. As a matter of good practice and to enhance the transparency of the joint marketing scheme in accordance with "Guidance on the Collection and Use of Personal Data in Direct Marketing" issued by PCPD in October 2010, OCL should consider taking steps to make prior announcement of such schemes to customers, e.g. by mailing to its customers information leaflets describing the nature and subject of each scheme.

9. **The privacy compliance monitoring processes against business partners and merchants should be strengthened.**

Onsite compliance checks have been performed by SDR/RMD since 2002 to ensure that security controls have been applied by business partners and merchants. Upon the completion of the site visit, SDR/RMD would prepare the "Site Visit Report", which included an overview of the assessment, findings and recommendations. Findings and recommendations would be communicated to the business partners and merchants where management responses would also be obtained. Follow up and review on remediation would be performed by SDR/RMD in the next onsite review.

By inspection of the "Site Visit Report", it was noted that the report covered the following generic IT security control domains:

- Physical access control;
- Servers/database security;
- Network security;
- Remote access control;
- Development system and control;
- Backup and recovery;
- Maintenance and support; and
- Other areas.

In view of the importance of the personal data privacy, RMD should expand the scope of the site visit by assessing the design and implementation of data protection measures. Octopus Group should also request the business partners and merchants to conduct regular compliance audits by independent third parties to ensure the compliance of relevant regulatory requirements as well as the contractual obligations of corresponding business partners.

10. **The personal data to be passed to business partners for direct marketing purpose should be minimised.**

Subsequent to the corporate restructuring in 2006, the CRM business was transferred out of OCL and OCL was not then involved in the CRM business. Prior to the cessation of the sharing of personal data with third parties by other members of the Octopus Group in July 2010, business partners and merchants would raise customer personal data extraction request with particular criteria to the SAM for direct marketing of their products. The fields of the extracted customer personal data were documented in the "Customer Extraction Form" ("the Form"), including:

- Customer name;
- Phone number;
- HKID card number (partial/full);
- Date of Birth (partial/full);
- Email address;
- Mailing address;
- Gender; and
- Bank account/credit card number.

With reference to the following published documents, if Octopus Group carries out similar business activities in the future, only limited customer personal data should be passed to third parties in order to reduce the privacy risks associated with the sharing and use of customer personal data:

- Administrative Appeals Board made a decision on 19 August 2010 regarding Wing Lung Bank Limited v Privacy Commissioner for Personal Data [AAB 38-2009], it is determined that for the purpose of cross-marketing, the amount of personal data to be passed should be confined to name and telephone number.
- The "Guidance on the Collection and Use of Personal Data in Direct Marketing" issued by PCPD in October 2010 states that "the data to be transferred should be confined to contact data, e.g. name, address and telephone number, enabling the Partner Company to approach the customer. Transfer or disclosure of the customer's sensitive data such as credit card number and/or Hong Kong Identity Card number to the Partner Company should be avoided".
- Section 8.4(b) of the Code of banking Practice states that "Institutions should not, without the prescribed consent of their customers, disclose customers' names and addresses to companies which are not related companies within the same group for marketing purposes".

11. **Documents retention should be strengthened and all records in relation to legal due diligence performed, customer data extraction process, evidence of data purging and destruction conducted by third parties, and monitoring of compliance with the confidentiality and personal data protection measures performed by the recipients of the customer personal data should be properly retained as audit trails.**

Prior to the restructuring in 2006, documentations were prepared by OCL during legal due diligence review, customer data extraction process, site visit to the third parties, and monitoring of compliance with the confidentiality and personal data protection measures by the recipients of the customer personal data.

Legal Approval Forms were introduced in 2003 for evidencing the internal approval process of business agreements. On reviewing the agreements with the business partners, we confirmed that all agreements with business partners were reviewed by In-house Legal Counsel; however, certain Legal Approval Forms were not filed with the agreements.

Besides, starting from late 2005, formal data extraction process was implemented where Customer Data Extraction Form was used to record details of the extraction such as short description of data extracted, number of records extracted, and data recipient. However, no records or documentation of data extraction was maintained prior to the period.

RMD performed onsite compliance checks supported by site visit reports since 2006. This practice is to ensure that proper security control measures were performed by Business Partners. No proper records were maintained for monitoring compliance on the Business Partners prior to this period.

Complying with personal data protection regulations, business partners were required to purge Octopus cardholder personal data regularly and emails confirmations were provided to Octopus Group upon completion of the purging exercise. The evidence of the purging and email correspondences was not fully recorded by Octopus Group.

In order to establish formal audit trails, proper documentation on compliance and monitoring of the data extraction and legal due diligence process should be maintained. Retention policy should be defined to ensure that customer personal data is properly retained or purged when necessary. The documentation records should also be reviewed regularly by the management to establish compliance and completeness of the process.

12. **The existing personal data extraction and transfer approval and logging process should be supported by system automation to ensure completeness of requests and extraction records with an effective monitoring mechanism.**

From 2002 - 2006, OCL was involved in the CRM business. Personal data passed to business partners was extracted from the first generation of the CRM System. The specialist data team in SAM was responsible for controlling the extraction process, which was performed at the user workstations.

In late 2005, subsequent to the launch of Rewards program and the upgrade of the CRM System, Octopus Group established the data extraction process. Upon the extraction was performed by Planning Team of SAM through the dedicated CRM workstation, the responsible staff was required to provide a manual Customer Data Extraction Form (the "Form") in recording details of the extraction including short description of data extracted, number of records extracted, and data recipient.

The Form would be passed to senior management of SAM and RMD for approval. The approved Form is submitted to Senior Manager of Infrastructure System Support Team, who then verifies the approvals and passes the extracted data to external business partners or relevant internal parties. A set of extracted files were saved at a common location of the file server. The only way to ascertain the volume and details of data extracted was to rely on this repository and the Forms, which were manually controlled.

In view of the sensitive nature of the data extraction process of personal data, it is important to maintain a highly reliable mechanism to record all requests, approvals and logs of such processes to ensure all data extraction tasks are properly approved where all of the extracted data are under proper consent. Therefore, Octopus Group should consider implementing an automated system to track all data extraction requests in order to ensure the completeness of the Forms and maintain an audit trail of the personal data extractions. Therefore, compliance with the PDPO and relevant regulatory requirements could be effectively monitored where irregularities could be promptly detected and reacted. Also, mandatory data fields and necessary approvals would be obtained in a systematic way through the automated process.

Besides, the extracted data files should be verified against the Form to ensure that the extracted data is the personal data required by the data requestor. A system log should also be maintained on the CRM system and reconciled to the Form to prevent against and detect any unauthorised extraction. The above controls allow the management to review and monitor the data extraction and transfer process.

Collection of Personal Data

13. OCL should improve the existing data collection process, such that the purpose of the collection is clearly stated and the manner of the collection is widely accepted by the general public.

Currently, OCL collects customer's personal data via various registration forms and application form (collectively, the "Forms"):

- Personalised Octopus Application Form;
- Octopus AAVS Application Form; and
- Friends of Octopus Registration Form.

After filling in the personal information by the customer, the Forms are submitted physically and/or electronically to OCL. The following personal information may be collected during the process by the Forms:

- Chinese and English name;
- HKID card number/passport number/birth certificate number;
- Gender;
- Email address;
- Date of birth;
- Contact number;
- Residential address; and
- Language preference.

The customer is required to sign the Forms to declare and confirm that all information provided to OCL is true, accurate and complete to the best of his/her information, knowledge and belief. The customer is also required to confirm that he/she read and understood the T&C as enclosed in the Forms, namely:

- Terms of Application for Personalised Octopus;
- Octopus Automatic Add Value Agreement; and
- Terms and Conditions for "Friends of Octopus".

The purpose for which the data are to be used, and the class of persons to whom the data may be passed were communicated to the customer through the description and T&C in the Forms. The Forms and its T&C are revised and reviewed by In-house Legal Counsel regularly against relevant laws and regulatory requirements, including PDPO.

Taking into account the latest suggestions on related good practices stated in the interim report issued by PCPD, as well as the principles laid down by the recent Administrative Appeals Board decision in August 2010, Octopus Group may consider enhancing the manner in which customer personal data should be collected, including:

- Collection of personal data;
- Personal data necessary for enjoying the basic benefits;
- Font size of the application form;
- Bundled consent;
- Use of personal data;
- The purpose and the class of transferee that will use the data;
- Options for customer to elect not to receive any direct marketing materials; and
- Further disposals of the data by third parties;

PCPD published a revised Guideline on the Collection and Use of Personal Data in Direct Marketing in October 2010 to help data users comply with its guidelines and regulations when using personal data for direct marketing activities. Octopus Group should, for any use of customer personal data in the future, observe and comply with PCPD's revised guideline, as well as the recommendations included in the final report for PCPD's investigation.

14. OCL should restrict the display of customer personal data in OCHS batch and summary enquiry.

OCHS was developed to perform a centralised clearing hub among merchants and banks. It also stored Octopus cardholders' personal information including the customer HKID number and payment account information. OCHS provides enquiry function to Operation staff in handling customers' card lost cases and data access requests. Security controls such as disallowing users to perform wildcard enquiry of customer records were implemented. Also, the USB port, CD drive, outgoing email and Internet access of the users' workstations were disabled so that the users cannot export any sensitive data by through removable storage and the Internet.

However, OCHS could provide batch and summary enquiry of customer records. The enquiry results displayed on screen include a batch of HKID number. Since the data can be easily viewed on screen, customer personal data may be exposed by unauthorised parties.

As OCHS handles customers' personal information, sensitive personal data, in particular HKID number, should be partially masked during on-screen enquiry of batch or customer summary in order to minimise the risk of leakage of personal information. Unmasked customer personal information should be displayed only in the detailed page of the customer record.

15. Detailed control procedures on data retention and destruction should be enhanced to ensure the compliance with the established retention period policy for personal data.

OCL has developed "Information Classification and Handling Guideline" and "Personal & Customer Data Protection and Privacy Procedures", which included the destruction procedures of customer personal data upon the expiry of data retention period. Besides, "Record Retention Period for Personal Data" was developed to highlight and specify the retention period of documents and records which involved customers' personal data. However, it was noted that the "Record Retentions Period for Personal Data" did not cover all types and formats of customers' personal data, such as OCHS generated reports and Friends of Octopus related documents. Besides, the detailed retention requirements, such as security safeguards and baseline, were not clearly stated.

To ensure the proper compliance with the retention period policy, the relevant policy should be enhanced to cover all types and formats of customer personal data records. Besides, control procedures of data retention should be clearly specified, in order to ensure that the data was stored no longer than necessary.

16. Octopus Group should segregate the use of personal data of Octopus Cardholders and Octopus Rewards Program Member stored in CRM system.

The CRM system was developed and implemented with centralised data warehouse and data mining capability as an alignment with the Expansion Strategy developed in early 2002. The CRM system was further upgraded in 2006 in order to support the target marketing part of the ORL business.

Customer personal data from both Octopus cardholder database and Octopus Rewards Program database are stored in different tables within the CRM system, where SAM Planning Team could access and perform the data extraction. However, there are no audit trails in ascertaining which table the personal data was extracted from.

The use of OCL and ORL database should be restricted to designated personnel only. An audit trail should also be available to track the data extraction to prevent unauthorised access to customer personal data from the OCL and ORL database.

End