Deloitte.
德勤

Octopus Cards Limited

Addendum to the Final Report on the Independent Assessment under Section 59(2) of the Hong Kong Banking Ordinance: 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.

Data Storage and Retention

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

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/cn/en/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 170,000 professionals are committed to becoming the standard of excellence.

About Deloitte China

In China, services are provided by Deloitte Touche Tohmatsu and Deloitte Touche Tohmatsu CPA Limited and their subsidiaries and affiliates. Deloitte Touche Tohmatsu and Deloitte Touche Tohmatsu CPA Limited are, together, a member firm of Deloitte Touche Tohmatsu Limited.

Deloitte China is one of the leading professional services providers in the Chinese Mainland, Hong Kong SAR and Macau SAR. We have over 8,000 people in 14 offices in Beijing, Chongqing, Dalian, Guangzhou, Hangzhou, Hong Kong, Macau, Nanjing, Shanghai, Shenzhen, Suzhou, Tianjin, Wuhan and Xiamen.

As early as 1917, we opened an office in Shanghai. Backed by our global network, we deliver a full range of audit, tax, consulting and financial advisory services to national, multinational and growth enterprise clients in China.

We have considerable experience in China and have been a significant contributor to the development of China's accounting standards, taxation system and local professional accountants. We also provide services to around one-third of all companies listed on the Stock Exchange of Hong Kong.