

Interim report on the investigation concerning personal data collected and disclosed under the Octopus Rewards Program

BACKGROUND

- 1 A compliance check against the Octopus group of companies in relation to the management of their customers' personal data was carried out in May 2010.

- 2 In response to the mounting public concern regarding the handling of personal data under the Octopus Rewards Program ("**the Program**") run by Octopus Rewards Limited ("**ORL**"), a company wholly owned by Octopus Holdings Limited ("**OHL**"), I gave notice pursuant to section 38(b) of the Personal Data (Privacy) Ordinance, Cap. 486 ("**the Ordinance**") to commence investigations against OHL and ORL on 22 July 2010 to ascertain whether there have been contraventions of the requirements under the Ordinance, including but not limited to Data Protection Principle ("**DPP**") 1 and DPP3 and section 34 of the Ordinance.

- 3 For the purpose of the investigations and pursuant to section 44(1) of the Ordinance, I summoned :
 - (i) Ms Prudence CHAN, Chief Executive Officer of OHL and Director of ORL,
 - (ii) Mr Edward KOPP, Chief Executive Officer of CIGNA Worldwide Life Insurance Company Limited ("**CIGNA**"), and
 - (iii) Ms TSANG Pik Yan, Grace, Authorized Representative of Card Protection Plan Limited ("**CPP**"),to attend before me and give information relevant to the investigations. Both CIGNA and CPP are transferees of the personal data of the members under the Program.

- 4 Examination of Ms CHAN, Mr KOPP and Ms TSANG took place on 26 July 2010 by way of a public hearing at the Office of the Privacy Commissioner for Personal Data on the 13th Floor of 248 Queen's Road East, Wanchai, Hong Kong.

- 5 As at the date of this interim report, the investigation is continuing and additional information and evidence are still being collected.

- 6 Since the investigations concern the personal data privacy of two millions plus individuals who have registered as members under the Program, I consider it appropriate to issue this interim report to keep the public informed of the progress of the investigations and to make timely suggestions on good practice to the parties concerned and other data users who may be engaged in practices similar to those engaged by ORL and OHL. In doing so, the public should be able to take precautions before giving out their personal data, and recommendations are offered to data users generally to take prompt actions to remedy or improve their personal data management in dealing with promotion activities.
- 7 I also wish to stress that this interim report is based upon the information available to me as of now after the hearing. The observations and comments made in this interim report are subject to review as the investigation progresses.

PROGRESS OF THE INVESTIGATION

Collection of personal data

- 8 At the hearing, Ms CHAN told me that the principal business of ORL is to run the Program. Under the Program, members could earn reward \$ every time they make a purchase from ORL's "business partners". A member will earn reward \$ upon the presentation of his registered Octopus card, and the reward \$ earned by a member may be used to redeem certain goods and services at ORL's "redemption partners" ("**the Basic Benefits**").
- 9 In order to become a member under the Program, it is a necessary condition that the applicant is a holder of an Octopus card, and he has to complete a registration form ("**the Registration Form**") designed and provided by ORL.
- 10 In the Registration Form, an applicant is requested to supply 16 items of information to ORL. The requested information is divided into two parts, namely "My Information" and "My Other Information". Certain fields in the Registration Form are also marked by asterisk which, according to the description at the top of the Registration Form, means that the fields are "Required Fields". Particulars of the requested information are summarized below :

“My Information”

The Required Fields marked by asterisks are :-

- (1) Octopus number appeared on an Octopus card
- (2) English name appeared on Hong Kong Identity Card / Passport / Birth Certificate
- (3) Hong Kong Identity Card numbers or Passport / Birth Certificate numbers
- (4) Gender
- (5) Month and Year of Birth
- (6) Contact mobile and Home / Office numbers
- (7) Home address

Other fields not marked with an asterisk are :-

- (8) Chinese name as appeared on Hong Kong Identity Card / Passport / Birth Certificate
- (9) Email address

“My Other Information”

- (10) Language preferred in communication (Chinese or English)
- (11) Marital status (Single or Married)
- (12) Education level (Primary, Secondary, University, Post-graduate, or Others)
- (13) Occupation (Self-employed, Housewife, Professional / Manager / Executive, Clerical / Administration, Civil Servant, Technical, Student, Retired, or Others)

- (14) Monthly Personal Income (No income, \$8,000 or below, \$8,001 - \$15,000, \$15,001 - \$25,000, \$25,001 - \$35,000, \$35,001 - \$50,000, or \$50,000 above)
- (15) Monthly Household Income (No income, \$10,000 or below, \$10,001 - \$20,000, \$20,001 - \$40,000, \$40,001 - \$60,000, \$60,001 - \$80,000, or \$80,000 above)
- (16) Interests (Sports, Beauty, Fashion, Fitness & Healthcare, Travel, Movie / Music, Dining Out, Investment, Personal Education, Computer / IT Products, Audio & Video Products, or Driving)

Personal data necessary for enjoying the Basic Benefits

- 11 I note from Clause 2.3(a) of the Terms and Conditions of the Octopus Rewards Program (“**T&C**”) printed on the Registration Form that, apart from the Basic Benefits, “Benefits” under the Program include promotions and other carefully selected offers that a member may receive from ORL or its “business partners” (“**Additional Benefits**”). Clause 3.3 of the T&C also provides that a member may opt out of receiving direct marketing materials from ORL or its “business partners” by notifying ORL by phone.
- 12 Based on the available information, it seems that under the Program a member may choose to receive only the Basic Benefits, and the Additional Benefits are optional. When being asked at the hearing, Ms CHAN confirmed that a member might elect not to receive any direct marketing materials.
- 13 When asked at the hearing whether it would be feasible for ORL to provide the Basic Benefits to a member if ORL was only provided with the applicant’s name and his Octopus card number, i.e. requested items (1) and (2) only, Ms CHAN answered in the affirmative.
- 14 It is clear that in operating the Program, for members to enjoy the Basic Benefits, ORL needs only collect an applicant’s name and his Octopus card number.

Bundled Consent

- 15 Applicants are required to sign the Registration Form in order to be registered as members under the Program. Only one space in the Registration Form is provided for an applicant's signature. In attesting his signature, an applicant not only signifies his intention to be registered as a member under the Program, but would also be taken as his declaration that :-
- (a) he has read and understands the T&C and agrees to be bound by them which may be amended by the ORL from time to time; and
 - (b) he agrees that upon his successful registration under the Program, his personal data provided in the Registration Form will be associated with his Octopus card and that he understands and agrees with the notice relating to Personal Data (Privacy) Ordinance contained in Clause 6 of the T&C.
- 16 Clauses 6.3 and 6.4 of the T&C are important because they contain the applicant's agreement on how their personal data supplied to ORL can be dealt with.
- (1) Under Clause 6.3, an applicant agrees to let ORL use all his personal data for 10 different purposes including, (i) providing him with offers, promotion and benefits by ORL, its subsidiaries, its affiliates and / or its business partners; (ii) designing new or improving existing services provided by ORL, its subsidiaries and its affiliates for customers' use; and (iii) as a source of information and data for other related purposes.
 - (2) For the purpose of Clause 6.3, an applicant is deemed to have agreed under Clause 6.4 that ORL may transfer or disclose data held by ORL relating to the applicant to any third parties which are under a duty of confidentiality to ORL including its subsidiaries, its affiliates and its business partners, whether within or outside Hong Kong.
- 17 The scope of permutable transferees of an applicant's personal data is tantamount to giving ORL a complete discretion. What is more, as admitted by Ms CHAN at the hearing, under the T&C an applicant would have no idea who those transferees could be.

- 18 It is plain that the applicant's agreement to subscribe for the Basic Benefits is bundled with his consent to ORL's use of his personal data. An applicant who only wishes to receive the Basic Benefits but does not want direct marketing materials from ORL or its business partners would have to sign the Registration Form first and opt out later. Ms CHAN said at the hearing that ORL would need 3 working days to process an opt-out request. That being the case, ORL can use an applicant's personal data for direct marketing purpose for a minimum period of 3 working days.
- 19 It will have to be conclusively determined whether it is fair for ORL to seek bundled consent from applicants in the circumstances.
- 20 I wish to advise applicants to carefully read the Registration Form and the T&C and decide whether their contents are agreeable to them before proceeding to sign the Registration Form. However, as the data user, ORL should ensure that applicants are adequately informed of their rights and obligations under the Program.
- 21 The final report of this investigation will include a determination on whether ORL has taken practical measures to ensure that the applicants are aware of the possible use of their personal data by ORL. In this connection, the specificity of the purposes of use and of the classes of transferees of the personal data, and the size of the font used in the Registration Form, are matters to be taken into consideration.
- 22 While a final decision has yet to be made on whether ORL has contravened a requirement under the Ordinance, I have the following comments on the Registration Form and suggest that ORL should consider them seriously :-
- (1) Applicants should be clearly informed that in joining the Program, he may elect to receive only the Basic Benefits;
 - (2) If the applicant so elects, he should be clearly informed that only his name and the Octopus card number are required;
 - (3) The applicant should be given an informed choice to authorize his personal data to be used for direct marketing purpose, i.e. opt-in choice;

- (4) Where the collection of particular items of personal data are optional, it should be clearly stated in the Registration Form;
- (5) Any contractual provisions that may have impact on the applicant's personal data privacy should be in a font that is reasonably readable by the general public without optical aids;
- (6) The classes of person to whom an applicant's personal data could be transferred should be reasonably specific; and
- (7) The personal information collection statement should also be in an appropriate font size readable by general public without optical aids.

Use of Personal Data

23 Ms CHAN told me at the hearing that since the operation of the Program, ORL had transferred members' personal data to 6 companies. Except for CIGNA and CPP whose contracts concerned were still subsisting, ORL had already terminated the contracts with the other 4 companies.

Transfer to CIGNA

24 ORL has provided me with a copy of the Cooperation Agreement between ORL and CIGNA dated 1 March 2009 ("**the Cooperation Agreement**"), but it is by no means a complete copy because various parts of it had been obliterated. In particular, all words under the following headings had been redacted :-

- (1) Commission
- (2) Performance Bonus
- (3) Persistency Bonus
- (4) Annual Fee
- (5) CRM Service Fee
- (6) Annual Minimum Revenue Guarantee
- (7) Forward-Paid Marketing Partnership Incentive

25 As described in Clause 10 of the Cooperation Agreement, these are payments in the forms of fees, commission and bonuses which may be payable to ORL

in relation to the performance of its obligations under the Cooperation Agreement.

26 One of ORL's obligations is found in paragraph 3.1 of the Cooperation Agreement, which provides that "*ORL is required to provide to CIGNA a list (the "Customer List") of [words or figures omitted] in each Contract Year based on the selection criteria set out in Appendix...*" Ms CHAN told me at the hearing that the redacted part refers to a minimum headcount (人次) of 750,000 and the Customer List contains the following personal data of applicants :

- (1) Names
- (2) Contact telephone number
- (3) Octopus card number
- (4) First 4 digits of Hong Kong Identity Card number
- (5) Month and year of birth
- (6) Partial mailing address (the street and name of the building)
- (7) Occupation
- (8) Salary Range
- (9) Gender
- (10) Duration of membership under the Program
- (11) Education level
- (12) Customer's spending under the Program

27 Clause 3.4 of the Cooperation Agreement also provides that "*If ORL cannot provide CIGNA with [words or figures omitted] customer counts in any Contract Year, the Annual Minimum Revenue Guarantee of the relevant Contract Year shall be reduced by the proportion that the unqualified customer counts shall bear to the total customer counts provided in that Contract Year.*"

28 Mr KOPP of CIGNA stressed that under the Cooperation Agreement, CIGNA was engaging ORL as its insurance agent. CIGNA was not paying ORL for transferring members' personal data to it, but for the services rendered by ORL in selling CIGNA's insurance products / services to members under the Program. However, it is apparent that ORL's income would largely depend upon the number of members whose personal data are transferred by ORL to CIGNA. This is plainly a transaction which the commodity is members' personal data. This may have a bearing on the

genuine nature of the Program. However, ORL does not seem to have made this known to the applicants.

- 29 It should not be presumed that ORL can transfer to any third party *all* the personal data an applicant has given it in all direct marketing activities. ORL as a data user should not in any one case disclose more personal data in excess of the purpose concerned.
- 30 In the present case, ORL not only provided names and contact telephone numbers to CIGNA, but also other information that does not seem to have relevance to the selling of insurance products. When asked at the hearing, Mr KOPP said that the information is necessary for selection of suitable products for promotion. The question why CIGNA needed to know the Hong Kong Identity Card number, occupation and spending data of an applicant in making direct marketing approach need to be answered substantially.
- 31 At the hearing, I asked both Ms CHAN and Mr KOPP questions about what they called a “secondment” arrangement under Clause 4.7 of the Cooperation Agreement, which provides that “*CIGNA shall second Telemarketers to ORL for making the Marketing Calls for and on behalf of ORL at no cost to ORL.*”.
- 32 The ordinary meaning of the term “secondment”, as I understand it, is an arrangement whereby an employee of a department or a company is sent to another department or another company for a short period of time. They remain the employee of the company at all material times. However, both Ms CHAN and Mr KOPP told me that their “secondment” did not require CIGNA to send employees to ORL’s office. What they did in gist was that ORL would send a list of members to CIGNA, whose telemarketer would make direct marketing calls to the members of the Program “in the name of ORL”. In other words, they are authorized by ORL to represent themselves as ORL’s staff.
- 33 I am very much concerned that while members receiving the marketing calls do not know about this sort of “secondment” arrangement, they may not even be aware that their personal data had already been transferred to CIGNA and they were in fact dealing with CIGNA’s staff. This arrangement may adversely affect the members’ right to object in a timely

fashion to the transfer and to the further collection of their personal data by CIGNA during the direct marketing process. I consider that in the process, members of the Program were deceived. I was told by Ms CHAN and Mr KOPP that ORL and CIGNA had ceased this “secondment” arrangement as from early July 2010. I would strongly advise ORL, being the data user not to adopt a similar practice with another organization again because of the potential adverse effect on the data subjects.

- 34 Notwithstanding the contractual provision that CIGNA must perform various obligations under this “secondment” arrangement in protecting members’ personal data transferred to it (e.g. ensuring that the telemarketers are fit and proper, and not to use the personal data for any other purposes, limiting access on a need to know basis, returning and purging of data, and preventing unauthorized access), I have not been provided with any evidence that ORL had performed due diligence in ensuring CIGNA’s obligations are fulfilled.

Transfer to CPP

- 35 According to Ms TSANG, the circumstances under which members’ personal data were transferred to CPP were different from that under CIGNA.
- 36 CPP’s participation in the Program started in June 2010. CPP has agreed to pay an annual fee to ORL which in return shall send promotion materials to its members by emails. A member who received the email would be asked to indicate his agreement to be approached by CPP by clicking an electronic button in the email.
- 37 ORL will compile a call list of those members who have agreed to be approached by CPP and the list will be sent to CPP. According to Ms TSANG, the list contains the following information of the relevant members :
- (1) Name
 - (2) Contact telephone number
 - (3) Gender
 - (4) Octopus card numbers
 - (5) Whether he is a traveler
 - (6) Whether he has previously lost his Octopus card

- (7) Whether he has subscribed to “Automatic Add Value Service” for his Octopus card
- (8) Whether he has credit card

38 Ms TSANG told me CPP had received two call lists comprising a total of around 7,200 members from ORL. After receiving the call lists, CPP would transfer the names, contact telephone numbers and gender to a telemarketing contractor, which made direct marketing calls in the name of CPP.

39 At the hearing, specific questions on the relevance of making direct marketing calls to members in respect of each data in the call list were raised to Ms TSANG. It seems to me at this stage that, in order for CPP to make direct marketing calls, certain personal data, e.g. whether the member has previously lost his Octopus card, may not be necessary. In the circumstances, whether ORL has disclosed excessive personal data to CPP is an issue to be determined at the conclusion of the investigation.

Further disposals of the data by CIGNA and CPP

40 As the supplier of members’ personal data, ORL should take practical measures to see that CIGNA and CPP do not use the personal data for purposes other than direct marketing their respective services and products under the Program, and the personal data shall not be further sold or transferred to other parties without restriction. ORL should also see to the deletion of the relevant personal data by CIGNA and CPP after use.

41 Both Mr KOPP and Ms TSANG confirmed at the hearing that CIGNA and CPP never transferred members’ personal data outside Hong Kong and that they would delete members’ personal data after conducting the direct marketing activities. However, the deletion is not verified by an independent third party.

42 CIGNA was required under Clause 4.7 of the Cooperation Agreement to take various steps in limiting access, prohibiting use other than for making marketing calls, and returning or purging of personal data. However, Mr KOPP said at the hearing that ORL had never required CIGNA to produce any report or confirmation certifying the performance of these contractual obligations.

43 Ms CHAN testified to the effect that ORL had asked CPP to destroy members' personal data after use and to confirm such destruction in writing. Ms TSANG on the other hand confirmed that members' personal data would be completely destroyed within 6 months.

44 Additional information to be provided by the parties concerned will be considered before a final conclusion is reached in the investigation on the adequacy of data protection by ORL of members' personal data transferred to CIGNA and CPP, I would strongly recommend ORL to consider taking the following steps in the future :

- (1) Before entering into any arrangement with a business partner to whom members' personal data would be legitimately transferred, to assess on the adequacy of data privacy protection offered by the business partner and where appropriate, a privacy impact assessment be conducted;
- (2) Specify in the agreement with the business partner that the transfer of members' personal data outside Hong Kong is strictly prohibited since the data are to be used in Hong Kong under the ORL;
- (3) Erasure of personal data held by the business partner be certified by a professional third party; and
- (4) Regular compliance audits be conducted on the implementation of data protection measures taken by the business partner.

Other comments

45 I have clearly stated at the hearing that I have no objection in principle to direct marketing activities. My concern has always been the proper management of personal data in relation to such activities.

46 Consumers' personal data are valuable for promoting businesses. Although the sale of personal data by a data user is not prohibited by the Ordinance, I would like the data subjects to be informed of the sale so that they can decide whether to give or withhold the giving of their personal data to the data user. These matters would be taken into account in determining whether the data user has contravened the requirements of the Ordinance.

47 On the other hand, consumers must bear in mind that they also have a part to play in the protection of their own personal data privacy. Consumer benefits are offered at all levels of marketing activities and one would not have any difficulties finding an offer that would seem most beneficial to him. In most, if not all, of these cases there are obligations or agreements on the part of the consumers which are embedded in the detailed terms and conditions in fine print in small-size leaflets. Before signing any of these documents, he is well advised to read them to ensure that such terms and conditions are agreeable to him.

PRELIMINARY FINDINGS AND RECOMMENDATIONS

Preliminary Findings	Recommendations
(1) It is feasible for ORL to provide the Basic Benefits to members of the Program if only the applicants' names and their Octopus card number are collected.	(1) ORL should clearly inform members that in joining the Program, they are entitled to elect to receive only the Basic Benefits. (2) If the applicant so elects, he should be clearly informed in the Registration Form that only his applicant's name and the Octopus Number are required.
(2) It is feasible for members under the Program to choose receiving only the Basic Benefits and not the Additional Benefits which are optional. ORL can make provisions for members to elect not to receive any direct marketing materials.	(3) Where the collection of particular items of personal data is optional, it should be clearly stated in the Registration Form.
(3) The applicant's agreement to subscribe for the Basic Benefits is bundled with his consent to ORL's	(4) The applicant should be given an informed choice to authorize his personal data to be used for direct

<p>use of his personal data in the T&C and cannot be segregated.</p>	<p>marketing purpose, i.e. consent should be expressed and not be deemed given.</p>
<p>(4) Clauses 6.3 and 6.4 of the T&C contain the applicants' agreement on how their personal data supplied to ORL can be used by ORL and they are printed in unreasonably small prints on the Registration Form.</p>	<p>(5) Any contractual provisions that may have an impact on the applicant's personal data privacy should be in a font that is reasonably readable by the general public without optical aids.</p>
<p>(5) The scope of permutable transferees of an applicant's personal data under Clauses 6.3 and 6.4 of the T&C is tantamount to giving ORL a complete discretion. An applicant would have no idea who those transferees might be.</p>	<p>(6) The classes of person to whom an applicant's personal data could be transferred should be reasonably specific.</p>
<p>(6) ORL's Cooperation Agreement with CIGNA is a transaction in which the commodity is members' personal data. CIGNA's telemarketer would make direct marketing calls to the members of the Program in the name of ORL. In this way, members of the ORL were not told that their personal data had already been transferred to CIGNA.</p>	<p>(7) As the existing practice may adversely affect members' right to object in a timely fashion to the transfer and to the further collection of their personal data by CIGNA during the direct marketing process, ORL should not adopt the same or a similar practice with another organization again.</p>
<p>(7) ORL not only provided names and contact telephone numbers to CIGNA but also supplied other information that does not seem to have direct relevance to the selling</p>	<p>(8) Generally speaking, only names and contact information are necessary for direct marketing purpose. ORL should not disclose other personal data</p>

<p>of insurance products.</p>	<p>which may be considered excessive.</p>
<p>(8) Further evidence is required to show whether ORL had performed due diligence in ensuring CIGNA's performance of its contractual obligations in protecting members' personal data that had been transferred to it (e.g. ensuring that the telemarketers are fit and proper, and not to use the personal data for any other purposes, limiting access on a need to know basis, returning and purging the data, and preventing unauthorized access).</p>	<p>(9) Before entering into any arrangement with a business partner to whom members' personal data would be transferred, ORL should assess the adequacy of data privacy protection offered by the business partner and where appropriate, consider making a privacy impact assessment by a professional third party.</p> <p>(10) Erasure of personal data held by the business partner be verified by a professional third party.</p> <p>(11) Regular compliance audits should be conducted on the implementation of data protection measures taken by the business partner.</p>
<p>(9) There was no contractual obligation under ORL's respective contracts with CIGNA and CPP restricting the transfers of members' personal data to places outside Hong Kong.</p>	<p>(12) Specify in the agreement with the business partner that the transfer of members' personal data to any place outside Hong Kong is strictly prohibited.</p>

Roderick B Woo
Privacy Commissioner for Personal Data
Dated 30 July 2010