

**Report Published under Section 48(2) of the
Personal Data (Privacy) Ordinance (Cap. 486)**

Report Number: R12 – 0080

Date issued: 11 October 2012



香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

The Collection and Use of Personal Data of Members
Under the Fun Fun Card Program run by
The China Resources Vanguard (Hong Kong) Company Limited

This report in respect of investigations carried out by the Privacy Commissioner for Personal Data (the “**Commissioner**”) pursuant to section 38(b) of the Personal Data (Privacy) Ordinance, Cap. 486 against China Resources Vanguard (Hong Kong) Company Limited is published in the exercise of the power conferred on the Commissioner by Part VII of the Personal Data (Privacy) Ordinance. Section 48(2) of the Personal Data (Privacy) Ordinance provides that “*the Commissioner may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report –*

(a) *setting out -*

(i) *the result of the investigation;*

(ii) *any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and*

(iii) *such other comments arising from the investigation as he thinks fit to make; and*

(b) *in such manner as he thinks fit.”*

Allan CHIANG
Privacy Commissioner for Personal Data

Background

Following the Octopus incident in October 2010, the Commissioner examined the collection and use of members' personal data under a number of prominent customer loyalty programs, including the "Fun Fun Card" program (the "**Program**") operated by China Resources Vanguard (Hong Kong) Company Ltd. ("**Vanguard**").

2. Consequently, the Commissioner initiated a formal investigation pursuant to section 38(b) of the Personal Data (Privacy) Ordinance (the "**Ordinance**")¹ against Vanguard to ascertain whether Vanguard had contravened the relevant requirements under the Ordinance.

Representations from Vanguard

3. In the course of investigation of this case, this Office collected information and evidence below from Vanguard.

The Program

4. The Program was launched and has been operated by Vanguard since 2000. Members were offered the following benefits:-

- (a) bonus points (1 reward point for every \$2 spent) for purchases made at Vanguard stores;
- (b) 5% discount on purchases of \$50 or above at Vanguard stores on 2nd, 12th and 22nd of every month; and
- (c) special discounts (through purchase and/or redemption of bonus points) provided from time to time on a range of selected products.

5. The name of the card issued under the Program was changed from "Fun Fun Card" to "Vanguard Rewards Card" in January 2012 [both cards are collectively abbreviated as the "**Card**"].

¹ The Personal Data (Privacy) Ordinance was substantially amended on 1 October 2012. However, for the purposes of this investigation, the applicable law at the material time was the version of the Personal Data (Privacy) Ordinance prior to 1 October 2012, which is referred to as the "Ordinance" throughout this report.

6. According to Vanguard, there was no ceiling for the bonus points stored in the Card and the bonus points were valid for one year from the date of purchase. Apart from use in special discount offers, the bonus points could also be redeemed for cash vouchers as follows:

- 2,500 bonus points = \$20 cash voucher
- 4,000 bonus points = \$50 cash voucher
- 6,000 bonus points = \$100 cash voucher
- 8,000 bonus points = \$200 cash voucher

Membership Application

7. When the Program was first examined by the Commissioner, there were two avenues for membership application. An applicant might complete a “Fun Fun Card Membership application form” (the “**Application Form**”) and submit it to any Vanguard store. Alternatively, the applicant might complete the electronic application form (the “**e-Application**”) available on the website of Vanguard (www.crvanguard.com.hk). The website also provided online service for existing members to check the balance of bonus points accumulated (the “**online service**”).

8. The Commissioner’s examination revealed two inconsistencies in the personal data collection practices between the Application Form and the e-Application:

- (a) The Application Form solicited 11 items of data² from the applicant including his full Hong Kong Identity Card (“**HKIC**”) number. The e-Application, on the other hand, required 12 items of data³, one of which was the first 5 characters of HKIC no. (i.e. A1234); and
- (b) The clause “*I also understand that CRV⁴ may use my personal information and records for the research and promotional purpose in*

² (1) Name in English and Chinese; (2) Gender; (3) Email address; (4) Contact number & mobile number, (5) Home Address; (6) Full date of birth; (7) Age group; (8) Education level; (9) Occupation; (10) Full HKIC number; and (11) Signature.

³ (1) Name in English and Chinese; (2) Gender; (3) Email address; (4) Contact number 1 & contact number 2; (5) Home Address; (6) Martial status; (7) Number of children / Age group distribution of children; (8) Year and month of birth; (9) Education level; (10) Occupation; (11) Personal monthly income/ number of family members/ family monthly income; and (12) the first 5 characters of HKIC number.

⁴ China Resources Vanguard (HK) Co. Ltd.

future.” was found in the Terms and Conditions (“**T&C**”) of the Program in the Application Form only. This clause was not found in the e-Application nor was there any clause to a similar effect.

9. Apart from these inconsistencies, neither the Application Form nor the e-Application contained a privacy policy or similar content with the effect of informing the applicants:

- (a) whether it was necessary or voluntary for the applicant to provide the data so required (Vanguard had failed to explain to the Commissioner during the investigation whether it was mandatory or voluntary for an applicant to provide Vanguard with each item of data in the application form);
- (b) the classes of transferees who may receive the data from Vanguard; and
- (c) how a member can gain access to and correct the data provided.

10. Regarding the purposes of collection of the data, the Commissioner only found one relevant clause on the use for research and promotion in the T&C of the Application Form (see paragraph 8(b) above). Tabulated below are the purposes of collection of each item of data provided by Vanguard during the investigation:

Table 1 – Purposes of collection of personal data by Vanguard

Item	Descriptions	Purposes
1	Name in Eng. and Chi.	Identification
2	Gender	Analysis and segmentation for different promotions
3	Email Address	Communication and promotion
4	Contact number	Identification and communication
5	Home Address	Communication and promotion
6	Marital Status	Analysis and segmentation for different promotions
7	No. of Children	Analysis and segmentation for different promotions
8	Date and Month of Birth	Analysis and segmentation for different promotions
9	Age Group	Analysis and segmentation for different promotions
10	Education Level	Analysis and segmentation for different promotions
11	Occupation	Analysis and segmentation for different promotions

Item	Descriptions	Purposes
12	Monthly household income (Range)	Analysis and segmentation for different promotions
13	Signature	To confirm that the applicant had read and understood the T&C and the Notice of the Program
14	HKIC number (Ceased to collect in January 2012)	Used as default password for log-in to the online service
15	Year of birth (Ceased to collect in January 2012)	Marketing analysis and promotions

11. Vanguard confirmed that there was no difference in the benefits offered to members whether their applications for subscription were made through use of the Application Form or the e-Application. The inconsistencies mentioned above arose as the e-Application was not updated in parallel with the Application Form. During the investigation, Vanguard took the initiative to suspend the e-Application as well as the online service. Up to 11 October 2012, neither the e-Application nor the online service has been resumed.

12. Vanguard submitted that it had never sold and had no plan to transfer members' personal data to other organizations for monetary gain. Also, Vanguard was the only party which may use and had used the members' personal data for research and promotion purpose.

Change in practice during the course of investigation

13. Apart from the suspension of the e-Application and the online service, Vanguard had revised the Application Form and the T&C therein. Also, a "Notice relating to the Personal Data (Privacy) Ordinance" (the "**Notice**") was added to the Application Form. These documents became effective from 1 January 2012.

14. According to the revised Application Form, the applicant is required to provide the following personal information (mandatory fields are asterisked):

- (1) Name in English and Chinese*
- (2) Gender*

- (3) Email address*
- (4) Contact number* (mobile / home / office telephone number)
- (5) Home address*
- (6) Marital status
- (7) No. of children
- (8) Date and Month of birth
- (9) Age group
- (10) Education level
- (11) Occupation
- (12) Monthly household income (Range)
- (13) Signature*

15. A comparison with the Application Form and the e-Application used when the Commissioner first examined the Program shows that Vanguard had ceased the collection of HKIC (whether in full or in part) and year of birth.

16. On the signature page of the revised Application Form, the applicant may indicate his/her wish not to have his/her name placed on Vanguard's marketing list by ticking the box provided.

The Notice

17. The Notice provides more details about the data collection purposes, classes of transferees who might receive the data and Vanguard's practice in handling data access as well as data correction requests. Up to 11 October 2012, Vanguard was still refining the Notice for the purposes of improving their compliance with the Ordinance. Reproduced below are the relevant extracts from the Notice:

- “2. From time to time it is necessary for members to supply us with the data in connection with the membership card application and the provision of other benefits and services. Data may be used and retained by us for the purposes of:*
- a. application, termination and renewal of the Vanguard Rewards Card membership;*
 - b. the daily management, operation and maintenance of the Program;*

c. *providing the services under the Program;*

...

5. *In accordance to the Ordinance ... all requests for access to or correction of Personal Data or information regarding policies and types of Personal Data held should be in writing and addressed to: ...”*

The revised T&C

18. Clause 6 of part II of the revised T&C stipulates that: *“Bonus points accrued to a member account cannot be transferred to other member’s account”*.

The Legal Requirements

19. The following provisions of Data Protection Principle (“DPP”)1 and DPP3 in Schedule 1 to the Ordinance, which were in force at the material time, are relevant to this investigation. DPP1 stipulated that:-

- “ (1) *Personal data shall not be collected unless–*
- (a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;*
 - (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and*
 - (c) the data are adequate but not excessive in relation to that purpose.*
- (2) *Personal data shall be collected by means which are -*
- (a) lawful; and*
 - (b) fair in the circumstances of the case.*
- (3) *Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that -*
- (a) he is explicitly or implicitly informed, on or before*

- collecting the data, of—*
- (i) whether it is obligatory or voluntary for him to supply the data; and*
 - (ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and*
- (b) he is explicitly informed—*
- (i) on or before collecting the data, of—*
 - (A) the purpose (in general or specific terms) for which the data are to be used; and*
 - (B) the classes of persons to whom the data may be transferred; and*
 - (ii) on or before first use of the data for the purpose for which they were collected, of—*
 - (A) his rights to request access to and to request the correction of the data; and*
 - (B) the name and address of the individual to whom any such request may be made,*

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.”

20. DPP3 provided that:-

“Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than-

- (a) the purpose for which the data were to be used at the time of the collection of the data; or*
- (b) a purpose directly related to the purpose referred to in paragraph (a).”*

21. The term “use”, in relation to personal data, was defined under section 2(1) of the Ordinance to include “disclosure” or “transfer” of the data.

22. According to section 2(3) of the Ordinance, “prescribed consent” meant “express consent of the person given voluntarily” which had not been withdrawn by notice in writing.

23. With regard to the collection of identity card number, paragraphs 2.1 to 2.3 of the “Code of Practice on the Identity Card Number and other Personal Identifiers” (“**PI Code**”) issued by this Office provide that:-

“2.1 Unless authorized by law, no data user may compulsorily require an individual to furnish his identity card number.

2.2 Without prejudice to the generality of paragraphs 2.1 and 2.3, before a data user seeks to collect from an individual his identity card number, the data user should consider whether there may be any less privacy-intrusive alternatives to the collection of such number, and should wherever practicable give the individual the option to choose any such alternative in lieu of providing his identity card number. Such alternatives may include but are not limited to the following:

2.2.1 the identification of the individual by another personal identifier of his choice;

2.2.2 the furnishing of security by the individual to safeguard against potential loss by the data user; or

2.2.3 the identification of the individual by someone known to the data user.

2.3 A data user should not collect the identity card number of an individual except in the following situations:

2.3.1 pursuant to a statutory provision which confers on the data user the power or imposes on the data user the obligation to require the furnishing of or to collect the identity card number;

2.3.2 where the use of the identity card number by the data user is necessary:

2.3.2.1 for any of the purposes mentioned in section 57(1) of the Ordinance (safeguarding security, defence or international relations in respect of Hong Kong);

2.3.2.2 for any of the purposes mentioned in section 58(1) of the Ordinance (the prevention or detection of crime, the apprehension, prosecution or detention of offenders, the assessment or collection of any tax or duty, etc.); or

2.3.2.3 for the exercise of a judicial or quasi-judicial function by the data user;

2.3.3 to enable the present or future correct identification of, or correct attribution of personal data to, the holder of the identity card, where such correct identification or attribution is or will be necessary:

2.3.3.1 for the advancement of the interest of the holder;

2.3.3.2 for the prevention of detriment to any person other than the data user; or

2.3.3.3 to safeguard against damage or loss on the part of the data user which is more than trivial in the circumstances;

2.3.4 *without prejudice to the generality of paragraph 2.3.3, for the following purposes:*

2.3.4.1 *to be inserted in a document executed or to be executed by the holder of the identity card, which document is intended to establish or to evidence any legal or equitable right or interest or any legal liability on the part of any person, other than any right, interest or liability of a transient nature or which is trivial in the circumstances;*

2.3.4.2 *as the means for the future identification of the holder of the identity card where such holder is allowed access to premises or use of equipment which the holder is not otherwise entitled to, in circumstances where the monitoring of the activities of the holder after gaining such access or use is not practicable; or*

2.3.4.3 *as a condition for giving the holder of the identity card custody or control of property belonging to another person, not being property of no value or of a value which is trivial in the circumstances.”*

The Findings of the Privacy Commissioner

Whether the collection of applicants' personal data was excessive

24. DPP1(1) of the Ordinance stipulated that a data user may not collect personal data unless the data is collected for a lawful purpose directly related to a function or activity of the data user. Moreover, the collection of the data must be necessary for or directly related to that purpose, and the data is adequate but not excessive in relation to that purpose.

25. According to Vanguard's representations, the Program was a customer rewards scheme whereby members benefited in the form of redemption of goods and promotional offers of discount. The Commissioner considers that the purposes of collection of the applicants' personal data as stated in Table 1 above

were directly related to the function of Program as stated in paragraphs 4 to 6 above. The Commissioner's views on the adequacy and excessiveness of the personal data collected are set out below.

Name (Item 1 of Table 1)

26. In view of clause 6 of part II of the revised T&C (see paragraph 18 above) that the bonus points cannot be transferred, the Commissioner is satisfied that, in order to provide the benefits or services under the Program to members, it is necessary for Vanguard to collect the name of an applicant.

Email Address, Contact number and Home address (item 3 to item 5 of Table 1)

27. According to Vanguard, these items were collected for the purposes of identification, communication and promotion. The Commissioner recognizes that email address (item 3), contact number (item 4) and home address (item 5) were collected by Vanguard to effectively communicate with members and to provide marketing material to them. Hence the Commissioner is satisfied that it is necessary for Vanguard to collect these items from an applicant.

Gender, Marital Status, No. of Children, Date of Birth (date and month), Age Group, Education level, Occupation, Monthly household income (Range) (item 2 and item 6 to item 12 of Table 1)

28. Given Vanguard is in the supermarket business selling a wide range of goods, its submissions that these data were collected for analysis and segmentation for different promotions is understandable. The Commissioner does not object that the information so required may enable Vanguard to better understand members' background and thus to make offers more suited to their needs. In the circumstances, the Commissioner is of the view that the collection of item 2 and item 6 to item 12 is directly related to the purposes of the Program and he has found no evidence to suggest that such collection is excessive.

Signature (Item 13 of Table 1)

29. According to Vanguard, the collection of signature was necessary for the

purpose of confirming that the applicant has read and agreed to the T&C of the Program. The T&C set out the rules and regulations on how the Program is operated. They form the basis of the agreement between every member and Vanguard. It is therefore important for the applicants to acknowledge that they abide by the T&C by signing the Application Form. The Commissioner is satisfied that the collection of signature serves a legitimate purpose and is not excessive.

HKIC number (Item 14 of Table 1)

30. Vanguard stated that the HKIC number was assigned as the default password for the online service of the website for the reason that it is unique information. Arguably, the same quality of uniqueness should also be achieved from assigning any six numbers or characters as the default password to an individual for identity authentication.

31. Paragraphs 2.1 to 2.3 of the PI Code set out the circumstances (see paragraph 23 above) under which collection of HKIC number is generally justified (e.g. *a doctor may require a patient's HKIC number to ensure that his past medical records are correctly attributed to him to enable proper treatment*). The collection of HKIC number for the purpose of assigning a default password for log-in does not appear to be justified under any of the specified circumstances under the PI Code.

32. In this case, the collection of HKIC number is not necessary and therefore excessive for the purposes of the Program. Should Vanguard resume its online service in future, Vanguard is advised to assign to individual members other numbers and characters as the default password.

Year of birth (Item 15 of Table 1)

33. Before the change in practice, Vanguard collected the age group (item 9) and year of birth (item 15) from the applicant. During the investigation, Vanguard did not give any view on whether these two data items duplicated each other as far as achieving the purposes of the Program was concerned.

34. In this regard, the Commissioner notes that the revised application form does not collect the applicant's year of birth and it is optional for an applicant to provide his/her date and month of birth.

35. To sum up, the Commissioner considers that Vanguard's collection of the applicants' HKIC number and year of birth was excessive for the purposes of the Program, contrary to DPP1(1).

36. However, the Commissioner is pleased to observe that, as mentioned in paragraphs 13 to 16 above, Vanguard had taken the initiative to revise the Application Form in the course of this investigation. The Commissioner is satisfied that the kinds of personal data to be collected under the Program in the revised application form (see item 1 to item 13 of paragraph 14 above) are commensurate with the purposes of collection, and are neither privacy intrusive nor excessive.

Whether the means of collection is lawful and fair in the circumstances of the case

37. DPP1(2) of the Ordinance required data users to collect personal data by means which are lawful and fair in the circumstances of the case. There is no evidence in this investigation that suggests the means of collection of the applicants' personal data under the Program by Vanguard was unlawful.

38. Given that one of the features of the Program is to promote the products and services of Vanguard, it should be within the reasonable expectation of the applicants that, upon becoming a member, promotional information and material relating to the products and services of Vanguard offered under the Program would be communicated to them.

39. The Commissioner is satisfied that Vanguard had not used any means that was unfair in the circumstances when collecting personal data from applicants of the Program. Hence there was no contravention of DPP1(2).

Whether the duty to inform data subjects was discharged

40. The Commissioner notes that Vanguard did not meet the notification requirement under DPP1(3) as mentioned in paragraph 9 above. When the Commissioner first examined the Program, there was no evidence to suggest Vanguard had, before the collection of membership applicants' personal data, informed the applicants whether the data was required on an obligatory or voluntary basis, the purposes of data collection (except for the purpose of research and promotion as mentioned in paragraph 10 above), and the classes of transferees. Also, there was no mention in the relevant documents as to whom members' data access and data correction requests should be addressed for handling. The Commissioner is therefore of the view that Vanguard had contravened DPP1(3).

41. Having said that, the Commissioner notes that during the investigation, Vanguard had developed the Notice to ensure the compliance with DPP1(3) (see paragraph 17 above).

Use of personal data

42. Vanguard stated that it had never disclosed or transferred members' personal data under the Program to any third parties for direct marketing purposes.

43. On the basis of the facts collected or made known, there is no evidence that indicates that Vanguard had used members' personal data under the Program in contravention of the requirement under DPP3.

Conclusion

44. In view of the foregoing, the Commissioner concludes that Vanguard had contravened the following requirements under the Ordinance:-

- (1) DPP1(1) for having collected applicants' "HKIC number" (in full in the Application Form and partially in the e-Application) for the purpose of providing applicants with default passwords for log-in to the online service of the Program;

- (2) DPP1(1) for having collected applicants' "year of birth"; and
- (3) DPP1(3) for having failed to take all reasonably practicable steps to ensure that applicants were notified of the matters required under DPP1(3).

Enforcement Notice

45. Pursuant to section 50(1) of the prevailing Personal Data (Privacy) Ordinance ("PDPO") and in consequence of an investigation, if the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the PDPO, the Commissioner may serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent any recurrence of the contravention.

Undertaking

46. On 26 September 2012, Vanguard provided the Commissioner with a formal undertaking to complete the erasure of HKIC and year of birth collected under the Program by 30 November 2012 and provide a written confirmation to this effect on or before 14 December 2012.

47. While Vanguard indicated that they had no plan to resume the e-Application and online service, the formal undertaking also included Vanguard's pledge that they would implement appropriate measures to ensure consistency of practice of personal data collection under the Program should the e-Application and the online service be resumed.

48. Although the Commissioner is of the opinion that Vanguard had contravened the requirements of DPP1(1) and DPP1(3) under the Ordinance, given the subsequent remedial actions taken by Vanguard, in particular, the introduction of the revised application form (which has incorporated the Notice) and the undertaking on the erasure of the HKIC numbers and the year of birth previously collected, the Commissioner considers that Vanguard has taken adequate steps to remedy the contravention. Accordingly, no enforcement notice has been served upon Vanguard in the present case.

49. However, the Commissioner has put Vanguard on **WARNING** that if it fails to observe the relevant requirements of the PDPO in similar situations in future, the Commissioner may consider taking enforcement action against Vanguard including the serving of an enforcement notice.

Other Comments

50. After the *Octopus* incident in 2010, public awareness of the collection and use of personal data in direct marketing activities was significantly raised. This investigation is one of the four investigations subsequently carried out in relation to customer loyalty programs.

51. The Commissioner is glad to see that Vanguard had on its own initiative taken steps to comply with the requirements of the Ordinance during the investigation. This sets a good example of a responsible data user who promptly remedied its non-compliant practice before the Commissioner had to resort to enforcement action against it. It is the Commissioner's expectation that after the *Octopus* incident, corporations in Hong Kong should have learnt a lesson and paid more attention to data privacy regulations.

52. With the enactment of the Personal Data (Privacy) (Amendment) Ordinance 2012, a tighter regulatory regime will be introduced in 2013 for the collection and use of personal data for direct marketing. The consequences of contravening the new requirements are dire. For example, if a data user fails to inform a data subject in an easily readable and understandable manner of its intention to use his personal data for direct marketing before it engages in the direct marketing activities, or if a data user fails to specify, in an easily readable and understandable manner, the classes of persons to which the data will be transferred for direct marketing before the data transfer, the data user commits an offence and is liable on conviction to a fine of \$500,000 and to imprisonment for 3 years.

53. Hence, the Commissioner would like to remind all organizational data users in Hong Kong to seriously review their privacy policies, personal information collection statements and data protection procedures to ensure compliance with the new provisions of the Amendment Ordinance.