

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

(English translation)

(This is an English translation of the Report compiled in Chinese. In the event of any conflict between this English version and the Chinese version, the Chinese version shall prevail.)

Report Number: R11-1982

Date issued: 20 June 2011



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

Transfer of Customers' Personal Data
Collected from On-street Promotional Activities by
Citibank (Hong Kong) Limited to a Third Party Insurance Company

This report in respect of an investigation carried out by me pursuant to section 38(a) of the Personal Data (Privacy) Ordinance, Cap 486 (“**the Ordinance**”) against Citibank (Hong Kong) Limited is published in the exercise of the power conferred on me by Part VII of the Ordinance. Section 48(2) of the 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

The Complaint

The Complainant was a credit card customer of Citibank (HK) Limited (“**the Bank**”). One day in May 2009, the Complainant received a call from an insurance company (“**the Insurance Company**”) promoting an insurance product (“**the Product**”) and the caller told the Complainant that the Insurance Company had obtained his personal data from the Bank. Being dissatisfied that the Bank had disclosed his personal data to the Insurance Company, the Complainant lodged a complaint with this Office.

Relevant Provisions of the Ordinance

2. Data Protection Principle (“**DPP**”) 1(3) and 3 of Schedule 1 to the Ordinance are relevant to this case.

DPP 1(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*
 - ...”*

DPP 3

“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).”*

3. Under section 2 of the Ordinance, the term “use”, in relation to personal data, includes “disclose” or “transfer” the data.

Information Collected during the Investigation

4. In the course of investigation of this case, this Office received written replies and relevant documents from the Complainant and the Bank respectively. Below are the relevant information and evidence collected by this Office.

Collection of the Complainant’s personal data by the Bank

5. According to the Bank, it collected the Complainant’s personal data in December 2008 when the Complainant applied for its credit card (“**the Credit Card**”) through an application form (“**the Form**”). The personal data provided by the Complainant included his English name, title (i.e. “Mr.”), identity card number, marital status, date of birth, nationality, address, residential telephone number, mobile phone number, occupation, job title, year of service and annual income.

6. The Bank stated that the Form contained the following provision:

*“By signing this application form, I/we (i) have read, accept and agree to be bound by that all terms and conditions (“**the Terms**”) of the Agreements (including the Credit Card contract, “**the Contract**”), the Policy Statement relating to the Personal Data (Privacy) Ordinance (“**Privacy Policy Statement**”)*

and this application form will constitute my/our agreement with you for the application for and the use of the Card(s); (ii) agree to jointly and severally abide by [the Contract] in the manner stated therein. ...I/We understand that the data requested is necessary for you to process my/our application and if I/we fail to provide the same to you, you may not be able to issue any card to me/us. I/We also understand that my/our data may be disclosed to, processed or kept by your service providers, and other classes of persons as set out in the Privacy Policy Statement in any country. I/We also understand that the Privacy Policy Statement form an integral part of this application form and shall be deemed incorporated into this application form, all contracts, account mandates and other binding arrangements which I/we have entered into or intended to enter into with you.”

The Bank stated that by signing the Form, the Complainant accepted and agreed to the above terms.

7. The Bank also stated that the Contract contained the following provision:

“...The Cardholder hereby agrees that all personal data relating to the Cardholder collected by the Company from time to time may be used and disclosed for such purposes and to such persons (whether in or outside Hong Kong) as set out in the Company’s policies and practices from time to time in force relating to personal data made available by the Company to its customers from time to time.”

Moreover, the Privacy Policy Statement stipulated that:

“(d) The purpose for which data relating to a Data Subject may be used by a Citi Entity or any person

who has obtained such data from the relevant Citi Entity are as follows:- ...(vi) marketing services or products of the Citi Entity and/or such selected persons; ...(xiii) purposes relating thereto.”

“(f) Data held by a Citi Entity relating to a Data Subject will be kept confidential but it may provide such information to:- ...(xi) selected companies for the purpose of informing Data Subjects of services which the Citi Entity believes will be of interest to Data Subjects.”

“(j) Data of a Data Subject may be processed, kept and transferred or disclosed in and to any country as the Citi Entity or any person who has obtained such data from Citi Entity referred to in (f) above considers appropriate. Such data may also be released or disclosed in accordance with the local practices and laws, rules and regulations (including any governmental acts and orders) in such country.”

Under the Privacy Policy Statement, “Citi Entity” is defined to mean “each of Citibank, N.A. Hong Kong Branch, Citibank (Hong Kong) Limited, Citicorp International Limited and Diners Club International (Hong Kong) Ltd.”

According to the Bank, the Insurance Company was one of the designated companies mentioned in paragraph (f) above. Under the above term, it could disclose the Complainant’s data to the Insurance Company.

8. Regarding when and how the Complainant was provided with the above documents from the Bank, the Bank stated that the Privacy Policy Statement was attached to every application form of the Credit Card. The Bank would also provide the Contract upon request by an applicant. The Bank stated that according to the Form signed by the Complainant, the Complainant got the Form from a salesperson of the Bank (“**the Staff Member**”) at an on-street promotional activity in mid December 2008.

However, the Bank had no information about when and under what circumstances the Complainant got the Form (together with the Privacy Policy Statement) from the Staff Member. Moreover, the Bank stated that according to its record, it approved the Credit Card in late December 2008 and issued a User Manual (“**the Manual**”) to the Complainant on the following working day, with the Contract and the Privacy Policy Statement attached. The Bank pointed out that the Contract stipulated that “*by signing or using the Card, [cardholders] ... agree or confirm their agreement to abide by ... the ... terms*” set out in the Contract.

9. The Bank provided this Office with a sample of the Manual with the attachment of the Privacy Policy Statement and a CD Rom, which contained the Terms (including the Contract).

Additional information provided by the Complainant

10. According to the Complainant, at about 6:30 p.m. on the incident date, he passed by an on-street promotional booth of the Bank. Attracted by the incentive of a promotion gift, he accepted the Staff Member’s promotion and applied for the Credit Card. The Complainant stated that as it was getting dark and he had presbyopia, the Staff Member filled in the Form for him. He signed on the Form as instructed by the Staff Member, who then photocopied his identity card. During the application process, the Staff Member had not mentioned/explained to him the Privacy Policy Statement, contents relating to the collection and use of personal data as stated in the Form, the purpose for which his personal data were to be used and the classes of persons to whom his personal data might be transferred by the Bank.

The Bank’s response to the information provided by the Complainant above

11. The Bank stated that as the Staff Member had resigned, it could not verify the above information provided by the Complainant.

12. The Bank reiterated that on or before the submission of the Form, the Complainant had already got the Form (together with the Privacy Policy Statement), and the Complainant’s signature on the Form indicated that he accepted and agreed to the relevant terms. The Bank also added that the Form had clearly cautioned “*PLEASE READ BEFORE SIGNING*”. As the

Complainant voluntarily signed and submitted the Form, he could not argue that he was not explicitly informed of whether it was voluntary for him to provide his personal data, the purpose for which the data were to be used, the classes of persons to whom the data might be transferred, and the fact that the Contract and the Privacy Policy Statement were legally binding on him.

Disclosure of the Complainant’s personal data by the Bank to the Insurance Company

13. The Bank confirmed that it had disclosed the Complainant’s data to the Insurance Company, including name, gender, date of birth, marital status, contact telephone number, correspondence address, credit card number, and the first 3 digits of identity card number (“**the Data**”).

14. The Bank stated that the Data were disclosed for the following reasons:

<u>Type of Data</u>	<u>Reasons for disclosure</u>
Name, gender	For addressing customers
Date of birth, correspondence address, credit card number, first 3 digits of identity card number	For identity verification
Marital status	For promotion of other appropriate products
Contact telephone number	For contacting customers

The business relation between the Bank and the Insurance Company

15. According to the Bank, the Insurance Company was not a related company of the Bank, but the Bank was the insurance agent of the Insurance Company. The Bank and the Insurance Company entered into an agreement (“**the Agreement**”) in 2008 for promotion of the Product.

16. Pursuant to the Agreement, the Bank was responsible for compiling a direct marketing call list of credit card and bank account customers who satisfied the selection criteria (“**the Promotion Targets**”), and passing the list together with the personal data of the Promotion Targets to the Insurance

Company, while the Insurance Company was responsible for carrying out telemarketing to the Promotion Targets. Under the Agreement, the Bank could receive commissions based on the premium of the Product paid by the Promotion Targets.

Findings of the Privacy Commissioner

Collection of the Complainant's personal data by the Bank

17. Regarding the collection of the Complainant's personal data by the Bank through the Form submitted by the Complainant, I have to consider whether the Bank had taken **all practicable steps** to **ensure** that the Complainant was explicitly informed, on or before the collection of his personal data, of the matters prescribed under DPP1(3), inter alia, the purpose (in general or specific terms) for which the data were to be used, and the classes of persons to whom the data might be transferred.

18. The Bank believed that it had complied with the requirements under DPP1(3) by notifying the Complainant of the matters prescribed in it. Its justifications were as follows:

- (a) On or before the submission of the Form, the Complainant was given the Form and the Privacy Policy Statement (in Chinese and English), which explicitly stated that the Bank had to obtain the required personal data before it could process the Complainant's application, or else the Bank would not issue any credit card to him; the purpose for which his personal data were to be used by the Bank; and the classes of parties to whom his personal data might be transferred.
- (b) The Complainant had signed the Form to confirm that he had read, accepted and agreed to be bound by the Terms and the Privacy Policy Statement; understood that the Privacy Policy Statement was an integral part of the Form and all the contracts signed between him and the Bank; and understood that the Bank might disclose his data to service providers in

any countries and other persons listed in the Privacy Policy Statement for processing and storage.

- (c) The Bank had cautioned the Complainant with the words “*PLEASE READ BEFORE SIGNING*” on the Form, while the Complainant still signed the Form voluntarily.

19. With regard to the Bank’s allegation that the Complainant had knowledge of the Terms, according to the information collected in the investigation, the Bank would only provide the documents containing the Terms (including the Contract) to customers upon request, or after the approval of their credit card applications. According to the Complainant, he had not taken the initiative to ask the Staff Member. Therefore, it appears that the Complainant was not informed of the Terms on or before the collection of his personal data by the Bank.

20. Even if the Complainant was provided with any document, in view of his eyesight problem, age and the fact that the incident took place in an on-street promotional activity in a winter evening, I consider that under these circumstances, it was difficult for the Complainant to carefully read, consider and understand the cautionary note, declaration and terms in the relevant documents and the Privacy Policy Statement.

21. Moreover, I have measured the font size used in the Bank’s Privacy Policy Statement which was attached to the Manual (issued to customers on the following day after their credit card applications were approved) and I found that the word height did not exceed 1.5 mm. I doubt how the Complainant could clearly read the terms of the Privacy Policy Statement.

22. In addition, the Complainant stated that the Staff Member had not mentioned and/or explained to him contents relating to the collection and use of personal data as stated in the Privacy Policy Statement and the Form at the material time, neither had the Complainant asked the Staff Member about this.

23. I note that the Privacy Policy Statement specified that “(d) *The purpose for which data relating to a Data Subject may be used by a Citi Entity or any person who has obtained such data from the relevant Citi Entity are as follows:- ... (vi) marketing services or*

products of the Citi Entity and/or such selected persons; ...(xiii) purposes relating thereto.” and “(f) Data held by a Citi Entity relating to a Data Subject will be kept confidential but it may provide such information to:-...(xi) selected companies for the purpose of informing Data Subjects of services which the Citi Entity believes will be of interest to Data Subjects.”. I consider that the companies, the services of which the Bank believed would be of interest to the applicants mentioned in paragraph (xi), could include different product or service classes (e.g. insurance companies, retailers for consumer products or medical organizations), but paragraph (f) above failed to explicitly inform applicants of which **classes** of organizations or persons that their personal data might be transferred to.

24. I consider that the intent of DPP1(3)(b)(i) is to require data users to provide reasonably sufficient information to let data subjects know the use of their personal data and the classes of persons to whom their data may be transferred by the data users. Data subjects can thus know whether the subsequent use of their personal data by the data users complies with the Ordinance. In the present case, irrespective of whether the Bank had provided the Complainant with the Privacy Policy Statement, the classes of data transferees were described in such liberal and vague terms that it would not be practicable for the Complainant to ascertain with a reasonable degree of certainty who could have the use of his personal data.

25. In sum, having considered all the circumstances of the case, I am of the view that the Bank has not taken **all practicable steps** to **ensure** that **on or before the collection** of the Complainant’s personal data, he was **explicitly** informed of the classes of parties to whom his personal data might be transferred. Hence it had contravened the requirement under DPP1(3)(b)(i).

Disclosure of the Complainant’s personal data by the Bank to the Insurance Company

26. With regard to the above disclosure, I first need to consider whether the Bank’s disclosure of the Complainant’s personal data to the Insurance Company for promotion of the Product (“**the Purpose of Use**”) was within the purpose of use for which the Complainant’s personal data were collected (“**the Collection Purpose**”) or directly related to the Collection Purpose. In

this regard, I consider that the crucial factors included the purpose of collection of the Complainant's personal data as conveyed to the Complainant by the Bank when the Complainant applied for the Credit Card, the reasonable expectation of the Complainant on the use of his personal data by the Bank, and applicable codes of practice, regulations or guidelines issued by relevant regulatory bodies on disclosure of customers personal data to third parties.

Whether the Disclosure was within the Collection Purpose

27. The Bank claimed that it had informed the Complainant through the Privacy Policy Statement of the purpose for which his personal data might be used, including marketing services or products of the Citi Entity and/or such selected persons. However, I note that the Bank could receive commission under the Agreement by disclosing customers' personal data to the Insurance Company for promotion of the Product. The Bank claimed that it was the agent of the Insurance Company and it received commission under the Agreement. From the Agreement, the Bank was responsible for compiling a direct marketing call list by selecting suitable customers according to the requirements of the Insurance Company, and passing the list together with the personal data of the Promotion Targets to the Insurance Company. The Insurance Company would be responsible for carrying out telemarketing. If a customer purchased the Product, the Bank would receive commission, which was a certain percentage of the premium paid by the customer in the first 12 months. If the customer renewed the insurance, the Bank and the Insurance Company would further assess the amount of the commission payable. From the above arrangement, I am of the view that the act of the Bank in disclosing customers' personal data for monetary gain was in substance sale of customers' personal data to the Insurance Company. This kind of commercial activity was obviously not within the purpose of use stated in the Privacy Policy Statement. I therefore find that the Purpose of Use was not within the Collection Purpose conveyed to the Complainant by the Bank.

Whether the Disclosure was directly related to the Collection Purpose

28. Although I find that the disclosure was not within the Collection Purpose, I still have to consider whether the Purpose of Use was directly related to the Collection Purpose. The reasonable expectation of the Complainant was a crucial factor in this regard.

29. When the Complainant provided his personal data to the Bank, his purpose was to apply for the Credit Card. The Complainant would only expect that his personal data in the Form would be used for the processing of his application for the Credit Card and future handling of his credit card account if his application was successful. Disclosure of his personal data by the Bank for the use specified in the Agreement was not within the reasonable expectation of the Complainant. After realizing that his personal data were disclosed to the Insurance Company, the Complainant felt dissatisfied and lodged a complaint with this Office. Such reaction of the Complainant showed that the disclosure was not within his reasonable expectation.

30. The decision of the Administrative Appeals Board (“AAB”) in a similar case, AAB No. 38 of 2009 (“**the Case**”), is helpful to me in determining whether the disclosure was directly related to the Collection Purpose:

“52. ...we consider that the sale and purchase between the Bank and CIGNA of Ms Wong’s data is not a purpose which has the prescribed consent from her. In our view, it is not one of the stated purposes included in paragraph 11(c) of the Agreement document provided to Ms. Wong.

53. As schedule 3 of the Cross-Marketing Agreement between the Bank and CIGNA indicated, both parties envisaged the sale and purchase of no less than 200,000 relevant data of the Bank’s customers within a 12-month period.

54. Relevant data is defined in the Cross-Marketing Agreement to mean the names and telephone numbers of the Bank’s customers. We failed to see how such kind of commercial activity is something that Ms Wong can be said to have already given her prescribed consent, just because she had received the application form and the Agreement. Such use of Ms Wong’s data is not the purpose for which it was first collected and its use by the Bank cannot be said to relate directly to the original purpose the data was collected, namely, the purpose was quite simply the application for a credit card and vetting of the applicant for the purpose of considering the application.”(emphasis added)

31. Having considered the above circumstances and in light of the

comments from AAB, I am of the opinion that the disclosure was outside the reasonable expectation of the Complainant, and thus not directly related to the Collection Purpose. Accordingly, DPP3 requires the Complainant's prescribed consent to be obtained for the disclosure.

Whether the Disclosure was with the Complainant's prescribed consent

32. In a similar vein, there are provisions in the Code of Banking Practice ("**the Code**") issued by the Hong Kong Association of Banks and DTC Association regulating the use of customers' personal data for marketing purpose by financial institutions. Under section 8.4(b) of the Code, financial 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.

33. As the Insurance Company is not a related company of the Bank, according to the requirement of the Code, the Bank should not disclose the Complainant's personal data to the Insurance Company unless with his prior prescribed consent. The Bank stated that based on the Terms and the contents of the Privacy Policy Statement, the Complainant had been informed of and had agreed to the disclosure of his personal data to the Insurance Company. I note the following sentences from the Form: "*I/We also understand that my/our data may be disclosed to, processed or kept by your service providers, and other classes of persons as set out in the Privacy Policy Statement in any country.*" In the circumstances, I have to further consider whether by signing on the Form which contained the above provision, the Complainant could be regarded as having provided his "prescribed consent" to the Purpose of Use.

34. With regard to prescribed consent, section 2(3) of the Ordinance stipulates that "*Where under this Ordinance an act may be done with the prescribed consent of a person (and howsoever the person is described), such consent means the express consent of the person given voluntarily; does not include any consent which has been withdrawn by notice in writing served on the person to whom the consent has been given.*" According to this requirement, prescribed consent has to be given expressly, not having raised any objection to the change of use of personal data does not constitute prescribed consent. Furthermore, prescribed consent has to be given

voluntarily. The person giving the consent has to clearly know what the consent is about.

35. I note that there was only one place for the applicant's signature on the Form for the application for the Credit Card. The Bank had not given customers a separate choice on whether they agreed to the transfer of their personal data to an unrelated company of the Bank for promotion of the latter's products. As a result, when customers signed the Form to apply for credit cards, they had to, at the same time, agree to *"my/our data may be disclosed to, processed or kept by your service providers, and other classes of persons as set out in the Privacy Policy Statement in any country."* In other words, applicants could only either give up the application or give bundled consent to the use when signing the Form (even though he finds such use objectionable).

36. Regarding obtaining customers' prescribed consent, AAB had the following comment in the Case:

"32. We believe that express consent should be given, as is normally the case, by for example inviting the customer to tick a box specifying whether the customer would agree to the possibility of using personal data for promotion by third party business."

37. The above comment made by the AAB supports my view that the "bundled consent" obtained by the Bank cannot be regarded as an express and voluntary consent, hence falling outside the definition of "prescribed consent".

38. In view of paragraphs 27 to 37 above, I am of the opinion that by disclosing the Complainant's personal data to the Insurance Company for marketing insurance products and earning commission, the Bank has contravened the requirements under DPP3.

Conclusion

39. In conclusion, I find that:

- (1) the Bank has contravened the requirement under DPP1(3) in

- relation to its collection of the Complainant's personal data;
and
- (2) with regard to the disclosure of the Complainant's personal data to the Insurance Company for marketing purpose, the Bank has contravened the requirement under DPP3.

Enforcement Notice

40. Pursuant to Section 50(1) of the Ordinance, I may serve an enforcement notice on the Bank if I am of the opinion that the Bank is contravening the requirements under the Ordinance or has contravened the requirements under the Ordinance in circumstances that make it likely that the contraventions will continue or be repeated. In other words, an enforcement notice will not be served if continued or repeated contravention of the Bank is unlikely.

41. The Bank confirmed to this Office in August 2010 that it had ceased disclosing customers' personal data to the Insurance Company for direct marketing purpose. Later, the Bank further stated that it had complied with the notice issued by the Hong Kong Monetary Authority on 12 August 2010 and ceased transferring customers' personal data to unrelated companies of the Bank for direct marketing.

42. The Bank further gave me a written undertaking ("**the Undertaking**") on 7 April 2011 that it will take the following actions:

- (1) The Bank will revise its Personal Information Collection Statement ("**PICS**") to the effect that:
- (a) The font size of the PICS is easily readable to individuals with normal eyesight;
 - (b) In its description of the purpose for which the data are to be used, it will be highlighted that the Bank may be remunerated in respect of the marketing of the services and products stated in the PICS; and;
 - (c) In its description of the classes of person to whom the data may be transferred, it will be highlighted that it would include "third party financial institutions,

insurers, credit card companies, securities and investment services providers” so that it would be practicable for customers to ascertain with a reasonable certainty how their personal data could be used and who could have the use of the data;

- (2) The Bank will cease the practice of sharing of the personal data of its existing customers with the Insurance Company or any unconnected third parties unless and until prescribed consent to such use is obtained from those existing customers;
- (3) In the event that the personal data of existing customers of the Bank would be shared with any business partners under any joint marketing program for monetary gains, prior prescribed consent to such use must be obtained from those existing customers;
- (4) The Bank will notify me in writing as and when it issues a new PICS (with revisions outlined above); and
- (5) The Bank will issue a written notice (“**the Notice**”) to the Insurance Company within 7 days from the date of the Undertaking, demanding it to delete and destroy all personal data of the Complainant that are in its possession within 1 month from the date of the Notice, and provide a copy of the Notice to me within 14 days from the date of the Undertaking.

43. In view of the matters presented in paragraphs 41 and 42, I am of the opinion that repeated contraventions of DPP1(3) and DPP3 on the part of the Bank in similar circumstances are unlikely. Therefore, an enforcement notice has not been served on the Bank.

Other Comments

44. I note that under the Agreement, the Insurance Company was responsible for conducting telemarketing to the Promotion Targets. However, apart from the contact information (name and telephone number) of the Complainant, the Bank disclosed his gender, date of birth, marital status, correspondence address, credit card number and the first 3 digits of identity card number to the Insurance Company. I am of the view that for the purposes of marketing insurance products and informing the Complainant of

the product information, disclosing the name and contact number of the Complainant to the Insurance Company would suffice. Furthermore, paragraph (f) (xi) of the Privacy Policy Statement stated that the purpose of disclosing customers' personal data was to provide data subjects with service information which would be of interest to them. In respect of this purpose, the disclosure of customers' personal data by the Bank other than name and contact number to the Insurance Company for marketing purpose was excessive.

45. The AAB shares my views in its following comment on the disclosure of the data by a bank to an insurance company for promotion of products in the Case:

“58. ... although a definition for relevant data is provided in the Cross-Marketing Agreement, more data than that was specified in the Banking Code in relation to a bank customer were transferred by the Bank to CIGNA which included address, gender, date of birth, partial identity card number and credit card number. We note that §8.4(b) of the Banking Code says without the prescribed consent of its customer, a bank should not disclose his/her name and address to a company which is not a related company to its Group for the purposes of marketing. It is not an advice that the Bank has complied with. The amount of personal data for the purposes of cross-marketing here was not confined to name and telephone number. We do not think it was right if there appears to be no safeguard a data subject has if there is simply no limit on the amount of personal data that can be legitimately transferred.”

Recommendations

46. I understand that business organizations may need to carry out on-street promotional activities as part of its marketing plan in order to successfully sell their services and products. This may involve the collection of customers' personal data, as in the present case in which the salesperson of the Bank filled in the credit card application form for the Complainant on the street. I note that in the circumstances, unless customers are specially reminded or given explanations, they may not understand the terms and

conditions in the form (including the terms of collecting and using their personal data) and this may lead to future disputes.

47. Through publication of this investigation report, I hope that business organizations conducting on-street promotional activities (which involve collection of customers' personal data) will take notice of their responsibility to inform customers of the purpose of collection of their personal data. This has to be done in ways which are clear and easily understandable to customers. In particular, they have to pay attention to the font size and layout of the PICS. I urge business organizations to provide appropriate and practicable assistance to their customers to help them understand the PICS, taking into account the circumstances of the promotional activity (e.g. the characteristics of their target customers such as age and education level, the on-site environment of the promotional activity such as crowd flow and lighting). Moreover, business organizations should have specific written policy in place to ensure that their staff will comply with DPP1(3) when collecting customers' personal data in promotional activities.

48. For collection and use of personal data in carrying out direct marketing activities (including through on-street promotional activities to collect personal data), business organizations should refer to "Guidance on the Collection and Use of Personal Data in Direct Marketing" we issued, which includes recommended good practices for protecting customers' personal data privacy.