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: R11-7946

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

Collection and Use of Customers' Personal Data by Industrial and Commercial Bank of China (Asia) Limited in Direct Marketing

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 Industrial and Commercial Bank of China (Asia) 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 customer of Industrial and Commercial Bank of China (Asia) Limited ("**the Bank**"). As the Complainant was dissatisfied that the Bank had called at her mobile phone number several times for direct marketing, she made a written request to a branch of the Bank ("**the Branch**") in 2008 requesting the Bank to cease using her mobile phone number for direct marketing. In response, the staff of the Branch confirmed to the Complainant that they would handle her request. Subsequently, the Complainant received one direct marketing call from an insurance company ("**the Insurance Company**") one day in April 2009 and another call from the Bank one day in June 2009. The Complainant believed that the Bank had not complied with her opt-out request ("**the Request**") and thus lodged a complaint with this Office.

2. As the Bank confirmed to this Office that it had transferred the Complainant's personal data to the Insurance Company for promotion of the Insurance Company's products, which involved disclosure of the Complainant's personal data by the Bank to a third party without her consent, thus the scope of this investigation also included whether the Bank had contravened the relevant requirements under the Ordinance for the collection and use of the Complainant's personal data.

Relevant Provisions of the Ordinance

3. Section 34(1) of the Ordinance, Data Protection Principle ("**DPP**") 1(3) and 3 of Schedule 1 to the Ordinance are relevant to this case.

Section 34(1)

" A data user who—

(a) has obtained personal data from any source (including the data subject); and

(b) uses the data for direct marketing purposes,

shall—

(i) the first time he so uses those data after this section comes into operation, inform the data subject that the data user is

required, without charge to the data subject, to cease to so use those data if the data subject so requests;

(ii) if the data subject so requests, cease to so use those data without charge to the data subject."

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-

...

(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

..."

DPP3

"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)."

4. 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

5. 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

6. According to the Bank, it collected the Complainant's personal data when the Complainant opened a general and investment account (personal) ("**the Account**") in March 2007 and applied for a credit card ("**the Credit Card**") in April 2008.

7. The Bank stated that a customer circular in relation to the Ordinance ("**the Circular**") was referred to in the application forms of the Account and the Credit Card and attached to the forms. It was stated in the application form of the Account ("**the Account Application Form**") that:

> *"…I/we hereby acknowledge that I/we have received and read a copy of the current version, and fully understood the provisions of these terms and conditions…*
>
> *…*
>
> *Circular to Customers and Other Individuals relating to the Personal Data (Privacy) Ordinance*
>
> *…*
>
> *I/We acknowledge and agree that my/our personal data will be used and disclosed in accordance with the Circular to Customers and Other Individuals relating to the Personal Data (Privacy) Ordinance.*
>
> *…*"

The Circular contained the following provisions:

> *"(4) The purpose for which data relating to a data subject may be used are as follows:*
>
> *…*
>
> *(ix) marketing services or products of the Bank and/or selected companies; and*
>
> *…*
>
> *(xvi) purposes relating thereto.*

(5) Data held by the Bank relating to a data subject will be kept confidential but the Bank may provide such information to the following parties for the purposes set out in paragraph (4):

...

(ix) selected companies for the purpose of informing data subjects of services which the Bank believes will be of interest to data subjects.

..."

8. Moreover, the Bank stated that the Complainant had signed the application form of the Credit Card ("**the Credit Card Application Form**") under the circumstances that "*I have read, understood and accepted the Declaration printed overleaf and the enclosed Major Terms and Conditions"*. In the Credit Card Application Form, item 8 of the Declaration section ("**the Declaration**") stated:

> *"...I/We also understand and agree that the Bank may use the information regarding me/us and/or my/our account with the Bank for marketing purposes and may exchange information with selected business partners for marketing purposes. I/We understand that I/we have the right to opt out of such marketing programs."*

Incident 1 : Transfer of the Complainant's personal data by the Bank to the Insurance Company

9. The Bank and the Insurance Company entered into an agreement in March 2009 in respect of a promotion program ("**the Program Agreement**"). According to the Program Agreement, the Bank would transfer the personal data of 17,500 credit card customers, including name, gender, telephone number, address, first 5 digits of identity card number and date of birth ("**the Data**") in 7 phases from March to September 2009 to the Insurance Company for promotion of the insurance plans of the Insurance Company. The Bank would also provide the name and address of those customers to a designated mailing company during the specified period for sending out direct mail ("**the**

Direct Mail"). According to the Program Agreement, the Bank could obtain certain fees from the Insurance Company (including the service fee for the purchase of the insurance products by the customers under the promotion program).

10. According to the Bank, it had sent the Direct Mail to the relevant customers (including the Complainant) in March 2009, informing them that representatives of the Insurance Company would contact them shortly and if they did not want to receive the promotion materials of the Bank, they could inform the Bank in writing.

11. The Bank stated that it had informed the Complainant of the use of her personal data by the Circular, and considered that the Complainant had authorized it to use her personal data for marketing purpose.

12. The Bank confirmed that it had directly uploaded the Data of the customers (including the Complainant) to the Insurance Company's database by encryption software in March 2009. The Bank explained that it had to transfer the Data to the Insurance Company for the following purposes:

(i) Name and address for sending direct mail;

(ii) Telephone number and gender for calling customers;

(iii) Date of birth for confirming customers' eligibility to purchase insurance; and

(iv) First 5 digits of identity card number (including alphabet) for verifying customers' identity.

13. Subsequently, a representative of the Insurance Company called the Complainant for promotion of its insurance product one day in April 2009.

Incident 2：Direct marketing call made by the Bank to the Complainant to promote medical check-up scheme

14. The Bank entered into an agreement with a private medical organization ("**the Medical Organization**") in April 2009. Under the agreement, the Medical Organization would offer a medical check-up scheme to the Bank's customers from April 2009 to March 2010, and the Bank was responsible for the promotion of the scheme to its customers and collection of

charges. The Bank confirmed that its staff member had directly called the Complainant one day in June 2009 to promote the medical check-up scheme of the Medical Organization. However, the Bank had not disclosed or transferred the personal data of its customers (including the Complainant) to the Medical Organization.

Non-compliance of the "opt-out request" by the Bank

15. According to the Bank, the staff of the Branch had faxed the Complainant's opt-out request submitted to the Branch in October 2008 to another branch where her account was maintained. After preliminary processing by the staff of that branch, the Request should be passed to the Branch Support Division of the Bank for follow up. However, due to its staff's negligence, this was not done. When the Complainant complained to the Bank by phone in December 2008, the Branch Support Division handled the Request. However, the Branch Support Division had not informed the Bank's Data Protection Officer of the Request. Thus the Complainant's data was not included in the master Do-not-call list maintained by the Data Protection Officer. It was not until April 2009 when the Complainant received the Insurance Company's direct marketing call and complained to the Bank by phone that the Bank completed the procedures of recording the Request in the system and updated the master Do-not-call list maintained by the Data Protection Officer.

16. Further, in June 2009, as a staff member of the Bank had neglected to follow the instruction of double checking the opt-out requests of the customers before calling the customers to promote the medical check-up scheme of the Medical Organization, a direct marketing call was made to the Complainant. In August 2009, the Bank confirmed to the Complainant in writing that she had been put on the opt-out list since April 2009.

17. The Bank stated that generally it would complete the handling of a customer's opt-out request within 7 working days.

Additional information provided by the Complainant

18. The Complainant stated that during the application for the Account and the Credit Card, the Bank had not briefed her the Circular or the

Declaration, nor informed her of the purpose for which her personal data were to be used and the classes of persons to whom her personal data might be transferred. Moreover, the Complainant said that when she opened the Account in March 2007, she had told the Bank's staff that she did not want to receive the direct marketing service of the Bank. The Bank's staff only replied that such request had to be made separately. Only when the Complainant enquired the Branch again did she know that customers had to make such request to the Bank in writing.

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

19. According to the Bank, the staff member who opened the Account for the Complainant ("**the Staff Member**") could not recall the exact circumstances on that day. However, in accordance with the usual practice, if a customer made any special request, the Staff Member would request the customer to make it in writing for follow up, but the Bank did not receive such request on that day. Moreover, the Bank believed the Staff Member would have followed its branch operation manual by providing new account customers with the Circular and briefed them the terms on the Account Application Form and the content of the Circular, and invited questions from customers. In relation to the Credit Card, the Bank pointed out that the Complainant applied for the Credit Card by mail, and the Complainant had not specified such request in the application document.

20. The Bank considered that as the Complainant had signed the Account Application Form and the Credit Card Application Form, the Complainant was legally bound by the terms therein. In this connection, the Bank quoted a court case[1] stating that when a person signed a document, even though he/she had not read the document or had not been explained of the content of the document, he/she would be taken to have agreed to the terms therein. Furthermore, the Bank considered that by signing the relevant application forms, the Complainant had, in law, voluntarily given express consent to the use (including transfer) of her personal data for the purposes specified in the terms. The Bank further quoted another case[2] to support its argument.

21. The Bank also quoted the section on collection of personal data in a

[1] Pearldelta Group Ltd v Huge Winners International Ltd [2010]HKEC 601.
[2] Shi Tao v Privacy Commissioner for Personal Data [2008] 3 HKLRD 332.

Guide for Data Users[3] issued by this Office in November 1996. Regarding the use (including transfer) of the Complainant's personal data, the Bank stated that by mentioning the use and disclosure of customers' personal data in the Account Application Form, the Credit Card Application Form and the Circular, it had taken practicable steps to ensure that data subjects were explicitly or implicitly informed of the relevant information in compliance of DPP1(3).

Findings of the Privacy Commissioner

Collection of the Complainant's personal data by the Bank

22. Regarding the collection of the Complainant's personal data in the Account Application Form by the Bank, though there were terms about collection and disclosure of customers' personal data in the Application Form, according to the information provided by the Complainant, during the account opening process, the Bank's staff had not briefed her the contents of the Circular or the Declaration, nor told her the purpose for which the Complainant's personal data were to be used and the classes of persons to whom the data might be transferred. On the other hand, the Bank believed that the Staff Member had explained the terms and the Circular to the Complainant according to its branch operation manual during the account opening process.

23. According to the information of the case, I could not ascertain whether the Complainant was provided with or was briefed on the Circular when she opened the Account. The Bank quoted the court case saying that when the Complainant signed the relevant application forms, she should be taken to have consented to the terms therein. However, unlike the situation in the case quoted by the Bank, data users are required under the Ordinance to take all practicable steps to ensure that the data subjects are explicitly informed of the purpose for which the personal data are to be used and the classes of persons to whom the data may be transferred.

24. In any event, even if the Staff Member had mentioned to the Complainant the provisions about the use and disclosure of customers' personal data in the Circular, the Complainant should only know that the Bank "*may*

[3] A Guide For Data Users No. 3, Outline Action Plan For Complying with the Data Protection Principles" November 1996 (ACTION 1 – Collect Personal Data Fairly).

provide [her] information to selected companies for the purpose of informing [her] of services which the Bank believes will be of interest to [her]". However, the companies selected by the Bank might belong to different classes. I consider that the provisions of the Circular could not explicitly inform the Complainant of the classes of persons to whom her personal data might be transferred. Furthermore, I find that the provisions of the Circular and the Account Application Form were printed in fonts of less than 1mm for English and less than 2mm for Chinese. Obviously, customers had to carefully go through the Circular to find out the provisions about the use and disclosure of customers' personal data.

25. A similar situation was considered in the Administrative Appeals Board ("**AAB**") No. 38 of 2009 where AAB made the following comments:-

> *"16. Whilst this Board does not wish to encourage people to sign a document without reading the content and only to rely later upon a non est factum plea, the very design of this application form in our view simply discouraged people from reading the fine print. It is also worthwhile to mention in s24.1(b) of the Code of Banking Practice issued by the Hong Kong Association of Banks (Hong Kong Banking code). It says credit card issuing banks are advised to print their terms and conditions in a size that is easy and clear to read.*
>
> *...*
>
> *22. ...The credit card in the present case was issued to Ms Wong as a consumer and not to a company or an individual in the context of negotiating commercial contract where greater care is expected. This is particularly relevant to our preliminary observation that the prints were so small that it discouraged applicants from reading the contents.*
>
> *23. We believe this distinction between consumer and business applicants may first be drawn as the Ordinance has its long title that it is "to protect the privacy of individuals in relation to personal data"...*
>
> *...*
>
> *27. One does not expect consumer customers to go from one clause*

to another in a small print document to find for themselves what was intended in relation to their personal data. This is not a reasonable expectation of what a consumer should do and must do. They are quite entitled to be drawn specific attention to the fact of being approached by other business companies. Personal particulars set out on an identity card form part of the "privacy" of a citizen and are protected by Article 39 of the Basic Law, Article 17 of the ICCPR and Article 14 of the Bills of Rights. An express waiver of such rights should therefore be sought before business promotion from third party companies could be made."

26. Regarding the Credit Card Application Form, I note that apart from item 8 of the Declaration mentioned in paragraph 8 above, there was no other provision about the use and disclosure of customers' personal data by the Bank. The selected business partners which would use customers' data for marketing purpose mentioned in the provision could belong to various different classes. Therefore, the provision could not explicitly inform the Complainant of the classes of "*selected business partners*" to whom her personal data might be transferred.

27. I consider that the intent of DPP1(3)(b)(i) of the Ordinance is to require data users to provide reasonably sufficient information to let data subjects know how their personal data would be used 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. Having considered the aforesaid circumstances and the comments of AAB, 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, she was **explicitly** informed of the classes of persons or organizations to whom her personal data might be transferred, thereby contravened the requirement under DPP1(3).

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

28. Regarding the Bank's disclosure of the Data of the Complainant to the Insurance Company for promotion of the insurance products of the Insurance Company ("**the Purpose of Use**"), I first need to consider whether the Purpose of Use was within the purpose 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 purposes of use conveyed to the Complainant by the Bank when collecting the personal data from her, the reasonable expectation of the Complainant on the use of her personal data by the Bank, and applicable codes of practice, regulations or guidelines issued by relevant regulatory bodies.

Whether the Purpose of Use was within the Collection Purpose

29. I note that the Bank disclosed to the Insurance Company personal data of credit card customers (including the Complainant) who had met certain criteria. As concluded in paragraph 27, 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, she was explicitly informed of the classes of persons to whom her personal data might be transferred.

30. Moreover, I note that under the Program Agreement, the Bank could obtain certain fees by disclosing its customers' personal data to the Insurance Company for promotion of its products, but the relevant provisions of the Circular and the Credit Card Application Form (e.g. "*exchange information with selected business partners for marketing purposes"*) did not mention that the Bank could benefit from the disclosure of customers' personal data. From the co-operation agreement between the Bank and the Insurance Company, the Bank would select target customers according to the criteria set by the Insurance Company and pass the personal data of the target customers to the Insurance Company, while the Insurance Company was responsible for telemarketing. The Insurance Company had to pay the "list rental fee" to the Bank. If the customers purchased any product, the Insurance Company had to pay the Bank a "service fee", which was calculated based on the amount of premium payable. From the above arrangement, the Bank had disclosed customers' personal data for monetary gain. I consider that such act 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 Circular or the Credit Card Application Form.

Whether the Disclosure was directly related to the Collection Purpose

31. Although I find that the Purpose of Use was not within the Collection Purpose, I have to consider whether the Purpose of Use was directly related to the Collection Purpose. In this connection, the reasonable expectation of the

Complainant on the use of her personal data by the Bank was a crucial factor.

32. When the Complainant gave her personal data to the Bank, her purpose was to open the Account and apply for the Credit Card. Having considered the provisions in the Circular and the Credit Card Application Form, I opine that even if the Complainant had noticed the provisions, she would not have expected the Bank would transfer her personal data to non-associated companies for benefit. In fact, the Complainant stated that after receiving the direct marketing call from the Insurance Company and confirming that it had obtained her personal data from the Bank, she immediately called the Complaint Division of the Bank to query why her personal data were sold to another company.

33. This situation was considered by AAB No. 38 of 2009 in which the following comments were made:-

> *"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 <u>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</u>, 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)

34. Having considered the above circumstances and in light of the comments from AAB, I am of the opinion that the disclosure of the Data of the Complainant by the Bank was outside the reasonable expectation of the

Complainant on the use of her personal data, 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

35. 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, "*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*".

36. As the Insurance Company is not a related company of the Bank, according to the requirement under the Code, the Bank should not disclose the Complainant's personal data to the Insurance Company unless with her prior prescribed consent.

37. In this regard, the Bank considered that the Complainant's signature on the Credit Card Application Form should be deemed to be her consent to the terms therein, and legally, the Complainant had voluntarily given express consent to the use (including transfer) of her personal data for the purposes specified in the Credit Card Application Form. In the circumstances, I have to further consider whether the Complainant's signature on the Credit Card Application Form could be regarded as the Complainant's "prescribed consent" to the Purpose of Use.

38. 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.*" Hence, 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.

39. I also note that there was only one place for the applicant's signature on the Credit Card Application Form. Regarding the transfer of customers' personal data to non-associated companies for marketing purpose and obtaining benefits in return, the Bank did not give its customers the right of a free choice. Thus, when customers signed the Credit Card Application Form, they had to *accept "…the Declaration printed overleaf (including exchange information with selected business partners for business purposes) and the enclosed Major Terms and Conditions"* indirectly.

40. The phrase "*exchange information with selected business partners for business purposes"* has not clearly explained the nature of the disclosure of the Complainant's personal data to the Insurance Company by the Bank. Furthermore, the Complainant's signature on the Credit Card Application Form represented a "bundled consent" obtained by the Bank and cannot be regarded as an express consent, hence falling outside the definition of "prescribed consent". In this regard, the decision of the AAB No. 38 of 2009, as indicated in the following comment, lends support to my views:

> *"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."*

41. As to the case[4] quoted by the Bank to support that it had obtained the Complainant's prescribed consent, I consider that the Bank had neglected the uniqueness of the facts of individual cases and applied the *Shi Tao* case to the present case by referring to the facts of that case and pointing out that the AAB agreed that the Appellant of that case had given prescribed consent by accepting the terms of service and the privacy policy statement. I note that the AAB made the decision based on the information presented to it at that time. In the present case, as the Bank had not taken all practicable steps to ensure that on or before the collection of the personal data, the Complainant was explicitly informed of the classes of persons to whom the data might be transferred, and the design and layout of the Circular and the Credit Card Application Form were not easily readable to individuals with normal eyesight, I consider that the Complainant was not clear about what the consent given in her signature was about. This does not fit into the definition of "prescribed consent". I am of the view that that part of the *Shi Tao* case quoted by the

[4] Shi Tao v Privacy Commissioner for Personal Data [2008]3 HKLRD332

Bank was not applicable to the present case.

42. The Bank quoted paragraph 155 of the judgment of the *Pearldelta* case, saying that as the Complainant had signed the Credit Card Application Form, even if she had not read the terms therein, she should be taken to have agreed to the terms. I reiterate that "prescribed consent" under DPP3 must be an express consent given voluntarily. In the *Pearldelta* case, the nature of the "Non est factum" defence was described in paragraph 150 as follows: *"if a party has been misled into signing a document essentially different from that which he intended to sign, he can plead non est factum in an action against him"*. Though I cannot ascertain whether the Complainant had been misled in the present case, the commercial act of disclosing the Complainant's personal data for monetary gain was obviously not within the reasonable expectation of the Complainant on the use of her personal data by the Bank. This was similar to the Australian case mentioned in paragraph 152 of the judgment of the *Pearldelta* case as follows: *"where a person signed a form in the belief it was a simple receipt, when in fact the document purported to extend an option to the sale of land"*. Based on the above analysis, I do not consider that the Complainant's signature on the Credit Card Application form was an express and voluntary consent.

43. In view of the above, I am of the opinion that by disclosing the Complainant's personal data to the Insurance Company for marketing insurance products and thereby obtaining benefit, the Bank has contravened DPP3.

Non-compliance with the opt-out request by the Bank

44. As regards whether the Bank has contravened section 34(1) of the Ordinance, I have to consider whether the Bank had ceased to use the Complainant's personal data for direct marketing after the Complainant requested the Bank not to do so.

45. It was not in dispute that the Complainant had made an enquiry in person at the Branch in October 2008 and had made the Request in writing. The Bank confirmed receipt of the Request, but due to its staff's negligence, the Request had not properly handled. When the Complainant complained to the Bank again, due to the fault of the Branch Support Division, the information of the Request recorded in the system had not been passed to the Data Protection Officer, leading to the transfer of the Complainant's personal

data to the Insurance Company for marketing purpose.

46. Moreover, after the Bank had finally completed handling the Request, the Bank's staff member who was responsible for marketing the medical check-up scheme of the Medical Organization failed to double check the opt-out requests in the system before calling customers, thereby leading to the direct marketing call about the medical check-up scheme of the Medical Organization being made to the Complainant.

47. I note that in handling the opt-out request of the Complainant, several mistakes were made by the Bank's frontline staff, the Branch Support Division and the marketing staff, and the Data Protection Officer also failed to spot the errors for rectification. Though the Data Protection Policy of the Bank contained the general requirements of handling opt-out requests, and the relevant guidelines also specified the procedures for handling opt-out requests, the above mistakes showed that handling of opt-out requests by the Bank was obviously inadequate. Moreover, I consider that it was not reasonable for the Bank to take as long as "7 working days" to complete handling of customers' opt-out requests (see paragraph 17 above).

48. In light of the above, I am of the view that the Bank had contravened section 34(1) of the Ordinance by failing to comply with the Request and thereby causing the Complainant's personal data being repeatedly used for direct marketing.

Conclusion

49. 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;
(2) with regard to the disclosure of Complainant's Data to the Insurance Company for marketing purpose, the Bank has contravened the requirement under DPP3; and
(3) the Bank has contravened section 34(1) due to non-compliance with the Complainant's opt-out request.

Enforcement Notice

50. 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 cannot be served if continued or repeated contravention of the Bank is unlikely.

51. In the course of the investigation, the Bank stated that the Insurance Company had deleted the Complainant's personal data. The Bank further gave me a written undertaking on 6 April 2011 that it will take the following actions:

(1) At the time of or before collecting personal data from applicants for bank accounts and/or credit cards, the Bank shall inform the applicants of the matters under DPP1(3)(b)(i) in writing (i.e. "**the Personal Information Collection Statement**" or "**PICS**").

The design and layout of the PICS (including font size and spacing) shall facilitate easy reading by customers with normal eyesight.

The PICS shall make reference to direct marketing of services or products of third parties (such as financial institutions, insurers, credit card companies, securities and investment services providers, reward, loyalty or privileges programme providers, and co-brand card partners (the names of the co-brand card partners can be found in the leaflet for the relevant card) of the Bank and its group companies), stating that the Bank may or may not be remunerated in respect thereof.

(2) As required by law, the Bank shall obtain customers' prescribed consent for sharing existing customers' personal data with a third party business partner for the latter's direct marketing use and obtaining remuneration in return.

(3) The Bank shall adopt a written policy or guideline ("**Guideline**") to ensure compliance with a customer's request to cease to use his/her personal data for the purpose of direct

marketing, and shall take all reasonably practicable steps, such as appropriate training, guidance and disciplinary actions, to ensure that its staff will comply with the Guideline.

(4) The Bank shall notify me of the effective date of the Guideline and provide me with a copy of the Guideline.

(5) The Bank shall include a section in its revised Circular, to provide a convenient means for customers, if they wish to do so, to notify the Bank that they do not wish to receive direct marketing promotions.

(6) The Bank shall send to its existing customers, together with its revised Circular, an explanation highlighting the changes including the additional clause regarding third party direct marketing for remuneration.

52. In view of the matters presented in paragraph 51, I am of the opinion that repeated contraventions of section 34(1), DPP1(3) and DPP3 on the part of the Bank in similar circumstances are unlikely. Therefore, an enforcement notice was not served on the Bank.

Other Comments

53. I note that in order for the Insurance Company to promote its insurance products to the Complainant, the Bank had disclosed to the Insurance Company the Complainant's Data including her name, gender, telephone number, address, first 5 digits of identity card number and date of birth. 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 information (i.e. telephone number and address) of the Complainant to the Insurance Company is already adequate. The Insurance Company may collect other personal data from the promotion targets when they have agreed to subscribe to the product. In light of the above, I opine that the Bank's disclosure of the Data to the Insurance Company for direct marketing was excessive.

54. My views are in line with the following comments in the decision of the AAB No. 38 of 2009:

"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

55. In the present case, the Complainant was disturbed by direct marketing calls due to the Bank's mishandling of her opt-out request. In fact, this Office often receives complaints from people who were disturbed by direct marketing activities in their everyday life. Through publication of this investigation report, I would like to remind business organizations of the importance of complying with opt-out requests under the requirements of the Ordinance. Under the Ordinance, a data user who does not comply with an opt-out request commits an offence and is liable on conviction to a fine at level 3 (maximum $10,000). Upon receipt of such complaints, I will consider the facts of the case and, as appropriate, refer the case to the Police for prosecution.

56. When carrying out direct marketing activities, business organizations should refer to "Guidance on the Collection and Use of Personal Data in Direct Marketing" issued by this Office, which provides guidance on managing the opt-out requests made by customers under section 34 of the Ordinance and recommended good practices to keep an opt-out list.

57. From a broader perspective, the Bank's non-compliance with the Complainant's opt-out request had shown the inadequacy of the opt-out approach under section 34 of the Ordinance. Under the current regime, data subjects can only rely on the organizations which carry out direct marketing

activities to comply with their opt-out requests. In other words, if the organizations have no adequate measures in place to handle the opt-out requests, or cannot effectively monitor its marketing staff in the proper implementation of the measures, the existing provisions, short of criminal prosecution and conviction, are not effective to prevent data subjects from being disturbed by unwanted direct marketing activities.

58. It is noted that the Government will, as part of the proposals to amend the Ordinance, raise the penalty for contravention of section 34(1)(b)(ii) of the Ordinance from a fine of $10,000 to a fine of $500,000 and imprisonment for three years. This should enhance the deterrent effect.

59. To protect the consumers' right of self-determination on the use of their personal data, this Office's position is that an "opt-in" regime should be adopted in the long-run requiring direct marketers to seek their explicit consent for the use of personal data for direct marketing purposes. Given that it would take time for the direct marketers to shift to an "opt-in" regime and that unsolicited telemarketing calls are the most annoying nuisance to many consumers, this Office has proposed to the Government the setting up of a territorial-wide "Do-not-call" register on person-to-person telemarketing calls as an interim improvement measure for consumers to opt out of all unwanted telemarketing calls. This proposal can be implemented under the Unsolicited Electronic Messages Ordinance as an extension of the existing "Do-not-call" register operated by the Office of the Telecommunications Authority which covers fax, short messages and pre-recorded telephone messages. I hope that the Government will seriously and promptly pursue the proposal, in an effort to strengthen regulation to prevent or reduce misuse of personal data for direct marketing.