PERSONAL DATA PROTECTION COMMISSION

[2017] SGPDPC 16

Case No DP-1701-B0440

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012

And

BHG (Singapore) Pte. Ltd.

… *Organisation*

DECISION

BHG (Singapore) Pte. Ltd.

[2017] SGPDPC 16

Mr. Yeong Zee Kin, Deputy Commissioner — Case No DP-1701-B0440

15 November 2017

Background

1 An organisation's requirement to prevent the unauthorised disclosure or access of personal data under the Personal Data Protection Act ("**PDPA**") is not absolute in nature; in that the obligation is not automatically breached upon the occurrence of a data leak. This case provides a classic example of the application of this principle.

2 The Complainant, a customer of the Organisation, discovered that she had accessed the online BHG loyalty card account of another customer ("**Customer V**") of the Organisation after she changed the password to what she thought was her BHG loyalty card account. As a result, the name, gender, date of birth, race, marital status, income group (based on income range) and residential address (collectively referred to as the "**Personal Data**") of Customer V was inadvertently accessed by the Complainant.

Material Facts

3 The Organisation is a department store with various outlets in Singapore. It operates a loyalty card programme called the BHG

Rewards Card programme for customers who fulfil certain criteria (such as a minimum spend within an allocated period in order to qualify for the programme). Customers issued with a BHG Rewards Card earn points on purchases made at the Organisation's stores depending on the amount spent. These points can then be used to redeem shopping vouchers for use at the Organisation's stores. There are also other benefits in joining the BHG Rewards Card programme, such as exclusive promotions and activities.

4 Both the Complainant and Customer V met the prerequisites for joining the BHG Rewards Card programme and applied to join the programme on 26 December 2016.

The BHG Rewards Card registration process

5 Customers who wish to register for the BHG Rewards Card programme are required to make their application at the Customer Service Counter ("**CSC**") at the Organisation's stores. The registration is generally done by the customer on the Organisation's electronic tablets by inputting certain personal data into an electronic registration form. Amongst other personal details, the customer is required to provide his mobile phone number and email address. The customer's mobile phone number is used as the default User ID to access the customer's BHG Rewards Card account online.

6 When the customer is done keying the required personal data into the electronic form, an employee of the Organisation at the CSC will assist the customer to submit the details. This would generate a membership number and automatically "refresh" the screen; the details keyed in by the customer would no longer be displayed. The

membership number is used as the default password to access the customer's BHG Rewards Card account online.

7 As a precaution, the employee assisting the customer with the registration is required to also manually refresh the screen on the electronic tablet by closing the registration form and opening a fresh instance of the form before using the tablet again. The manual "refresh" procedure is also to be undertaken if there are any technical problems in using the electronic tablet for the registration.

8 The electronic tablet was also programmed to purge all the details keyed into the form if there was inactivity for about 30 seconds.

Accessing the customer's online loyalty card account

9 As set out above at paragraphs 5 and 6, a customer may access his BHG Rewards Card account online by using his mobile phone number as his User ID and the membership number as his password. If the customer forgets his membership number, he can request for a new password to be sent to his email address which the customer would have keyed in when registering for the loyalty card.

The registration of the Complainant's and Customer V's accounts were affected because of technical problems with the electronic tablets at the Jurong Point store

10 On 26 December 2016, both the Complainant and Customer V visited the Organisation's Jurong Point store and applied to join the BHG Rewards Card programme. On the same day, the Assistant Retail Manager (the "**Assistant Retail Manager**") of the Jurong Point Store who was tasked to assist customers in registering their BHG Rewards

Card accounts had experienced technical problems with the two electronic tablets used for registration. She informed the relevant department of the technical issues.

11 When the Complainant approached her for assistance in registering for the BHG Rewards Card, the Assistant Retail Manager handed the Complainant one of the electronic tablets ("**tablet 1**") to input the required details into the electronic registration form. However, technical issues caused the electronic tablet to "hang" or become unresponsive a few times when the Complainant tried to input the required details. The Assistant Retail Manager decided to abandon the electronic registration and instead asked the Complainant to fill in a physical registration form and subsequently issued the Complainant with a temporary BHG Rewards Card together with a membership number.

12 According to the Organisation, the technical issues experienced in typing the details into the electronic registration form was likely due to one or both of the following:

(a) The postal code directory uploaded onto the Organisation's registration system was not up to date. The system failed to recognise the postal code entered by the Complainant as her postal code was not included in the version which the Organisation was using at the time, causing the electronic tablet to "hang".

(b) Poor Wi-Fi connection on the day meant that the electronic tablet would have had difficulty connecting to the Organisation's registration system.

13 Customer V who was at the CSC at the same time as the Complainant was also having problems with the other electronic tablet ("**tablet 2**") which he was using to register for the BHG Rewards Card. A part time employee ("**Employee A**") of the Organisation who was also stationed at the CSC was assisting Customer V. Employee A asked Customer V to try using tablet 1 which was last used by the Complainant instead. However, when Employee A handed tablet 1 to Customer V, the screen was not refreshed properly and continued to display at least some of the Complainant's personal data. It is not known how much of the Complainant's personal data continued to be displayed, but as will be explained in the next paragraph, at least the mobile phone number and email address of the Complainant continued to be displayed.

14 Customer V proceeded to key the required details into the electronic registration form using tablet 1. However, Customer V's BHG Rewards Card account was registered with the Complainant's mobile phone number and email address. This is likely because the Complainant's mobile phone number and email address continued to appear on the form while Customer V was keying in his details. However, it is not clear why Customer V left the Complainant's particulars on the form or why he did not alert Employee A or any other employee to the fact that the Complainant's details were still visible on the form. Customer V was able to complete and submit his electronic registration and was issued a BHG Rewards Card account number.

The Complainant accesses Customer V's account information

15 On the same day, the Complainant downloaded the app ("**BHG App**") which allowed customers to access their BHG Rewards Card

accounts and tried to log into her account. As explained above at paragraph 9, the default login credentials to the BHG App were the mobile phone number registered with the customer's account (default user ID) and the customer's membership card account number (default password). Given that the Complainant's mobile phone number was tied to Customer V's BHG Rewards Card account number, the login credentials did not match and the Complainant was denied access to her account.

16 The Complainant, therefore, then submitted a password reset request to the Organisation by providing her mobile phone number and email address in accordance with the Organisation's password reset process. This password reset was successfully activated because the Complainant's mobile phone number and email address matched the details with which Customer V's account was registered. Once the password was reset, the Complainant managed to log into what she thought was her account. However, once she accessed the Account, the Complainant realised that, except for her mobile phone number and email address, the Account contained the personal data of Customer V. The Complainant alerted the Organisation and this office of this unauthorised access.

Commissioner's Findings and Basis for Determination

17 The issue to be determined in this case is whether the Organisation complied with its protection obligation pursuant to section 24 of the PDPA and implemented reasonable security arrangements to prevent the unauthorised access to the Personal Data.

18 For completeness, the Deputy Commissioner is satisfied that the 2 preconditions to the application of section 24 as stated in *Re Hazel Florist & Gifts Pte Ltd* [2017] SGPDPC 9 at [8] to [9] – that BHG (Singapore) Pte Ltd is an Organisation within the meaning of the PDPA and is in possession or control of the Personal Data – have been met and it is not in dispute that section 24 applies in this matter.

19 It is also not disputed that the information to which the Complainant had access, as set out above at paragraph 2, falls within the definition of "personal data" under section 2 of the PDPA as it was possible to identify Customer V from that information alone.

20 Further, it is not disputed that the Complainant was not supposed to have access to the Personal Data; the access was therefore without authorisation.

Whether the Organisation was in breach of section 24 of the PDPA

The security arrangements implemented by the Organisation to prevent unauthorised access to the Personal Data

21 The investigations by this office found that the following security arrangements were implemented by the Organisation to prevent unauthorised access to the Personal Data:

(a) Automated "refresh" of the screen: The electronic registration system was programmed such that the screen on the electronic tablet would "refresh" once the electronic registration form was successfully submitted. This would mean that the personal data keyed in by the customer would be deleted from

the registration form on the electronic tablet and would no longer be displayed on the screen.

(b) Manual "refresh" of the screen: The Organisation's staff assisting customers with their BHG Rewards Card registration at the CSC are required to "refresh" the system on the electronic tablet before they hand the electronic tablet to the next customer. This manual "refresh" is done by closing the open instance of the electronic registration system and opening a fresh instance of the system. The manual "refresh" is also required to be done whenever the staff encounter a technical issue with the electronic tablet. This manual "refresh" process and general guidance on handling customer's personal data was communicated to both the Assistant Retail Manager and Employee A through mandatory training programmes. The Assistant Retail Manager received on-the-job training sessions 3 days a week over a period of 10 months, which included training in the electronic registration of customers' BHG Rewards Card applications. Additionally, the Assistant Retail Manager was also trained by the Organisation's in-house trainer on the electronic registration process. Employee A also received on-the-job training on the electronic registration process. Both staff completed the training before the incident occurred.

(c) Login credentials for the BHG App: The default login credentials are set as a customer's mobile phone number (user ID) and membership card account number (password). Each customer who registers for the BHG Rewards Card will be assigned a unique 16-digit membership card account number that

is automatically generated from the Organisation's system once a registration is completed.[1]

(d) Authentication for password reset requests: A customer may request a password reset by providing the customer's mobile phone number and email address, as a form of verification and authentication by the system before a password reset is allowed.

(e) Automatic time-out: The electronic registration form is programmed to time out after about 30 seconds of inactivity, after which all the personal data keyed into the electronic registration form will be deleted.

The unauthorised access was caused by a confluence of events and circumstances that would have been difficult to foresee

22 The investigation determined that the unauthorised access was caused as a result of the following events and circumstances:

(a) The Complainant's electronic registration could not be completed meaning that the Complainant's data was not automatically cleared from the electronic registration form.

(b) Employee A did not correctly "refresh" tablet 1. In this regard the Assistant Retail Manager had handed tablet 1 to Employee A and asked her to perform a manual "refresh". The

---

[1] See *Re ABR Holdings Limited* [2016] SGPDPC 16 at [15] to [16], where it was held that the organisation's use of a single string of numbers as the only security arrangement to identify and authenticate access to personal data may constitute reasonable security arrangements depending on the sensitivity of the personal data protected only if the number is unique, unpredictable and reasonably well-protected.

Assistant Retail Manager had on numerous occasions during the same day asked Employee A to perform the manual "refresh" and checked that it was done properly. On this occasion, the Assistant Retail Manager, given that Employee A had performed the manual "refresh" properly on all of the earlier occasions and that the CSC was very busy during this peak period, trusted Employee A to perform the manual "refresh" and did not check if it was done.

(c) Customer V did not alert either Employee A or the Assistant Retail Manager and continued with his registration despite the Complainant's data continuing to be displayed. This, to the Deputy Commissioner's mind, is one of the baffling features of this case. Customer V did not provide his own mobile phone number and email address but left the contact details of someone else in an online form that he was filling out himself. There is a certain degree of responsibility that each person should exercise over his own personal data, even if this is no more than contact details that is freely disseminated. Customer V's oversight in this case was a key mistake in an unfortunate sequence of events.

(d) Of all the fields of personal data keyed in by the Complainant, only the Complainant's email address and mobile telephone number were included in Customer V's BHG Rewards Card account. Unfortunately, this was the exact information that allowed the inadvertent unauthorised access of the Personal Data.

23 The above explanation for the cause of the unauthorised access of the Personal Data shows that it was caused by a confluence of events

and circumstances. It is clear that the Organisation recognised its obligation to protect its customers' personal data and addressed its mind to the various scenarios in which the personal data of a BHG Rewards Card applicant could be disclosed or accessed without authorisation during the registration process. It recognised that the automatic "refresh" could potentially fail and as such the Organisation required its staff to perform a manual "refresh" as well. The requirement to perform a manual "refresh" and the process for doing so was communicated clearly to all staff assisting at the Organisation's CSCs. Besides the training programmes the Assistant Retail Manager and Employee A underwent, the senior staff at the CSCs also supervise the other employees in performing the manual "refresh" on a day-to-day basis. This supervision, which the Assistant Retail Manager performed during the day of the incident, served as another line of security during the registration process.

24 Finally, access to a customer's BHG Rewards Card account would only be granted if the user attempting to access the account knew the said customer's (i) mobile phone number; and (ii) the rewards card number or, in the case of a password reset request, the email address.

25 The question that remains is whether the above arrangements were reasonably appropriate in protecting the Personal Data from unauthorised access. In answering this question, the Deputy Commissioner notes that the wording of section 24 does not require an organisation to provide "*an absolute guarantee*"[2] for the protection of

---

[2] *Re Tiger Airways Singapore Pte Ltd and others* [2017] SGPDPC 6 at [17].

personal data in its possession or under its control and takes reference from the Advisory Guidelines on Key Concepts in the PDPA which recommends that:[3]

> "…[e]ach organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data."

26 In this case, the Personal Data, while important, were essentially demographic and contact details. In such circumstances, would the Organisation be required to implement security arrangements in addition to those that were already implemented at the time of the incident? Looking at the security arrangements that were implemented at the material time, it is clear that the automatic "refresh", the manual "refresh" and the supervisory checks would have all separately prevented the unauthorised access.

27 In this incident, however, the circumstances were such that each of these arrangements failed individually. First, both tablets 1 and 2 were not functioning properly during the day. Second, the Complainant's registration could not be submitted electronically and hence the electronic registration form was not refreshed automatically. Third, Customer V could not complete his registration with the tablet he was initially given and instead used tablet 1 immediately after the

---

[3] PDPC, Advisory Guidelines on Key Concepts in the PDPA (revised 27 July 2017) at [17.2].

Complainant's failed attempt to register using tablet 1. Fourth, Employee A did not properly perform a manual "refresh" of tablet 1 as was the process stipulated by the Organisation and as requested by the Assistant Retail Manager. This was despite Employee A performing the manual "refresh" properly numerous times during the day. Fifth, the Assistant Retail Manager failed to check that the manual "refresh" was done properly. Sixth, Customer V did not alert the staff at the CSC that the Complainant's personal details continued to appear on the electronic registration form, and did not replace the details but continued to submit his application with another person's mobile phone number and email address as part of his registration details. Seventh, the only details of the Complainant with which Customer V registered his account were the exact details which were required to allow the Complainant access to the Personal Data.

28 Looking at the above, it is the Deputy Commissioner's view that this incident resulted from an unusual confluence of circumstances. Also, nothing in the investigations pointed to a systemic problem that caused the unauthorised access to the Personal Data. This appeared to be a one-off incident that would have been difficult to foresee. Therefore, the Deputy Commissioner is of the view that the security arrangements implemented by the Organisation to prevent the unauthorised access of the Personal Data were reasonable in the circumstances.

Remedial Action by the Organisation

29 The Organisation launched an internal investigation into the unauthorised access of the Personal Data when the Complainant alerted

it to the incident. The Organisation undertook the following remedial actions:

(a) Responding to the affected individual: The Organisation informed Customer V of the unauthorised access to the Personal Data and created new membership accounts for the Complainant and Customer V with the correct sets of personal data;

(b) Remedial action concerning staff training: The Organisation scheduled refresher data protection training for all CSC staff and issued a warning to the Assistant Retail Manager for her contributory role in the unauthorised access of the Personal Data in order to deter the other CSC staff from deviating from the SOPs;

(c) Remedial action concerning technical safeguards: The Organisation instructed and scheduled its IT personnel to verify the setting of its electronic tablets at all of its outlets and carry out extensive checks on all its electronic tablets to ensure proper function and correct settings. It also informed its vendor of the technical problems faced in using the tablets. The Organisation also purchased and uploaded into its electronic registration system the most updated version of the postal code directory to prevent the same problem from recurring and provided every outlet with a new 4G Wi-Fi dongle to ensure a stable network connection; and

(d) Further remedial action on operational processes: The Organisation instructed its consultant to review the membership registration process to consider only collecting names, mobile

phone numbers and addresses in future registrations (with the collection of other personal data optional) and to study a potential revision of the verification process which grants customers access to their membership accounts via the BHG App, including stronger authentication checks before a customer is able to request for a password reset.

Conclusion

30 On balance, the Deputy Commissioner concludes that the Organisation implemented security arrangements of a reasonable standard to protect the personal data in its possession and under its control, and therefore makes a finding of no breach in the present case. Further, the Deputy Commissioner finds that the remedial actions undertaken by the Organisation satisfactorily addresses the residual harm caused by the unauthorised access to the Personal Data. There is, therefore, no need for the Deputy Commissioner to issue any directions in this case.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION