PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 36

Case No DP-1705-B0781

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

And

Singapore Telecommunications Limited

… *Organisation*

DECISION

Singapore Telecommunications Limited

[2019] SGPDPC 36

Tan Kiat How, Commissioner — Case No DP-1705-B0781

12 September 2019

Background

1 This case concerns a design issue in a previous version of Singapore Telecommunications Limited's (the "**Organisation**") "My Singtel" mobile app (the "**Mobile App**"), which resulted in the unauthorised disclosure of the personal data of the Organisation's customers. The current version of the Organisation's Mobile App does not have this design issue as it has been fixed.

2 On 17 May 2017, the Personal Data Protection Commission (the "**Commission**") received information from an anonymous informant alleging that there was a vulnerability in the Organisation's Mobile App, which allowed the informant to access the account details of other customers (the "**Data Breach**"). Following an investigation into the matter, the Commissioner found the Organisation to be in breach of section 24 of the Personal Data Protection Act 2012 ("**PDPA**"). The Commissioner sets out below his findings and grounds of decision.

Material Facts and Documents

3 The Organisation is a telecommunications company in Singapore. The Mobile App was developed by the Organisation's IT team to enable its customers to track their account information and manage add-on services. Communications between the Mobile App and the Organisation's servers are conducted via Application Programming Interfaces ("**API**").

4 The Organisation's customers can login to the Mobile App via the following methods:

(a) Mobile Station International Subscriber Directory Number ("**MSISDN**") login: where a customer's mobile phone is connected to the Organisation's mobile data network (3G/4G), the Organisation's servers will verify that the MSISDN and IP address of the mobile phones are correct before granting the customer access to the Mobile App;[1]

(b) One Time Password ("**OTP**"): through validation of the OTP sent to customers via SMS and entering it in the Mobile App ("**OTP Login Method**"); and

(c) OnePass: by using their OnePass login and password.

5 Customers that login to the Mobile App via the MSISDN or OTP login method have access to the following data relating to their own account:

[1] Each MSISDN is assigned a unique IP address. When a user logs in to the Mobile App via the MSISDN login method, the backend server will verify the MSISDN assigned to that IP address. Once verified, the login attempt will be deemed to be authenticated and the user will be granted access to the Mobile App.

(a) the mobile number used to access the Mobile App;

(b) related service plan information (i.e. data, talktime and SMS usage);

(c) outstanding bill amount;

(d) bill payment due date; and

(e) billing account number.

6 In addition to the data mentioned at paragraph 5 above, customers that login to the Mobile App via the OnePass method also have access to all the service information for all Singtel services registered under that Singtel OnePass ID. In addition, if such customers had opted for electronic billing, they would have access to the following data relating to their own account:

(a) the customer's name;

(b) the customer's billing address; and

(c) all Singtel services and corresponding usage (where applicable) under the same billing account number.

7 The anonymous informant claimed that the API on the server could be manipulated by using specialised tools to gain unauthorised access to the account details of other customers through the following methods:

(a) The MSISDN is a string of numbers that incorporates within it the customer's mobile phone number. By logging in using a legitimate Singtel account via the MSISDN login method and changing the value in the

MSISDN field (i.e. to another customer's mobile phone number)[2] that was sent from the Mobile App's API to the Organisation's servers, the informant was able to retrieve the account details (such as the billing account number and billing cycle) of the other customer.

(b) Thereafter, by logging in using a legitimate Singtel account via the OnePass method and changing the value in the billing account number and billing cycle fields, the informant was able to obtain the customer's bill, which contains further personal data such as the customer's name, billing address and all Singtel services and corresponding usage (where applicable) under the same billing account number[3].

8 The informant accessed four billing accounts and extracted the customer's name, billing address, billing account number, mobile phone number as well as customer service plans (including data, talk time and SMS usage). While there was no further evidence of unauthorised access, the personal data of approximately 330,000 of the Organisation's customers who were using the Mobile App at the material time were put at risk of disclosure.

9 Although the Organisation had engaged a third party security vendor to conduct regular security penetration tests on the Mobile App and backend systems (including the API), the tests had not detected the design issue in the API that led to the Data Breach and the Organisation was unaware of it.

---

[2] The subscriber's mobile phone number was used by the Organisation's servers to retrieve the subscriber's account and billing details.

[3] As mentioned at paragraph 6 above.

10 During the investigation, the Organisation admitted that the Data Breach was caused by a design issue in the API – the application input[4] was not validated against the login credential used to access the Mobile App before performing the requested operation (the "**Direct Object Reference Vulnerability**"). Because all request parameters sent by the Mobile App to the Organisation's server during a valid login session were assumed to be valid, once a user was legitimately authenticated to initiate a valid login session on the device (via the MSISDN, OTP or OnePass login methods), the user would be able to intercept and change the field parameters in the API requests between the Mobile App and the server. Notwithstanding, the Organisation asserted that such an action was "not something that a normal user of the App would attempt" and the attacker must be "technically competent" as the changing of the parameters could only be performed on a workstation.

11 Soon after it was notified of the Data Breach, the Organisation took remedial actions to resolve the Direct Object Reference Vulnerability. The Organisation enhanced the API in order to tightly couple the Mobile App user's identifiers to the authenticated session. In this manner, should the parameters be modified during the same authenticated session such that they do not match the Mobile App user's identifiers (e.g. the MSISDN field is changed to another number and service information such as data usage of that other number is requested), the user will see an error message and be logged out.

[4] Such as the MSISDN for the MSISDN or OTP login method, and the MSISDN, billing account number, billing payment due date for the OnePass login method.

The Commissioner's Findings and Basis for Determination

12 It is not disputed that the subscriber's name, billing address, billing account number, mobile phone number as well as customer service plans (including data, talk time and SMS usage) are "personal data" as defined in section 2(1) of the PDPA ("**Personal Data**"). There is also no dispute that the PDPA applies to the Organisation as it falls within the PDPA's definition of "organisation". The key issue to be determined in this case is therefore whether the Organisation had complied with its obligations under section 24 of the PDPA.

Whether the Organisation complied with its obligations under section 24 of the PDPA

13 Section 24 of the PDPA provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. It is not disputed that the Personal Data was in the Organisation's possession and/or control.

14 Having considered the material facts, the Commissioner finds that even though the Organisation had engaged a third party security vendor to conduct regular penetration tests on the Mobile App and backend systems (including the API), the Organisation failed to put in place reasonable security arrangements with respect to the said API to protect the Personal Data.

15 First, by the Organisation's own admission, the Data Breach was caused by the Direct Object Reference Vulnerability, which was a design issue in the API. The Organisation failed to take into account the risk of manipulation to the parameters sent from the Mobile App's API to the Organisation's servers when

designing the Mobile App. The validation of parameters (whether input or non-input fields), which could have prevented unauthorised access to the Personal Data, were not implemented as part of the API's initial design.

16 The Direct Object Reference Vulnerability is a relatively basic design issue and well-known security risk that a reasonable person would have considered necessary to detect and prevent. It was one of Open Web Application Security Project ("**OWASP**") 2013's top 10 most critical web application security risks and OWASP recommended, among other things, the usage of Indirect Object Reference as a prevention method.

17 Furthermore, as highlighted in the Commission's *Guide to Building Websites for SMEs* (at [6.5]), programmers should be aware of the common website vulnerabilities and adopt the appropriate programming techniques and practices to ensure that personal data cannot be exposed through such vulnerabilities. Although the *Guide to Building Websites for SMEs* sets out key considerations for the process of setting up a website, the same principles are similarly applicable when programming a mobile application. This is because the same issues arise when a server responds to requests from a mobile app as when it responds to requests from a web browser.

> "**6.5 Website Programming**
>
> 6.5.1 When programming the website, programmers should be aware of the common website vulnerabilities, and adopt the proper programming techniques and practices to avoid them. **Programmers can use the OWASP Top 10 vulnerabilities list as guide** and some common vulnerabilities include:

- Injection (e.g. SQL Injection)
- Cross-site scripting
- Buffer overflows
- **Poor authentication & session management**

6.5.2 **Organisations and any engaged IT vendors should ensure that personal data cannot be exposed, either accidently or by design, through any such vulnerabilities. The website functions should be thoroughly tested or scanned for vulnerabilities**, before the website is launched."

[Emphasis added.]

18 By failing to take into account the risk of manipulation to parameters sent from the Mobile App's API to the Organisation's servers, the Commissioner finds that Organisation subjected its customers to the risk of actual and potential unauthorised access of their personal data.

19 At this juncture, the Commissioner would like to deal with the Organisation's claim that exploiting the Direct Object Reference Vulnerability was "not something that a normal user of the App would attempt" and that the attacker must be "technically competent" as the changing of the parameters could only be performed on a workstation.

20 While the changing of parameters would require a person to have some knowledge of the tools and methods for doing so, anyone with working knowledge of how a mobile app communicates with the servers through an API could have exploited the Direct Object Reference Vulnerability. The tools and software required to manipulate the parameters are available online.

21 The Organisation was aware that direct object reference vulnerabilities had been discovered in its Mobile App. Despite having received professional advice to take precautions against such vulnerabilities, the Organisation omitted to conduct a full code review on the input and non-input fields and hence failed to discover the Direct Object Reference Vulnerability that was exploited in this case.

22 As mentioned at paragraph 9 above, the Organisation had engaged a third party security vendor to conduct regular security penetration tests on the Mobile App and backend systems.[5] The Direct Object Reference Vulnerability was not detected prior to the Data Breach but a variation of it was found in the October 2015 penetration test ("**2015 Penetration Test Report**") and rectified in November 2015. In the 2015 Penetration Test Report, the security vendor cited three examples of Direct Object References vulnerabilities in the API (collectively, the "**2015 DOR Vulnerabilities**").

23 During the investigation, the Organisation represented that the 2015 DOR Vulnerabilities were specific to the API accepting *input fields* (i.e. parameters keyed in by users at the user interface level), whereas the Direct Object Reference Vulnerability did not validate non-input fields (i.e. parameters not keyed in by users such as automatically generated URL at the backend). As the Organisation had only conducted a code review for the 2015 DOR Vulnerabilities on APIs accepting *input fields*, the Direct Object Reference Vulnerability that caused the Data Breach was not discovered at the time. However, contrary to the Organisation's representation, a review of the 2015 Penetration Test Report showed that both input and non-input fields were affected by the 2015 DOR

[5] At the time of the Data Breach, the most recent penetration tests on the Mobile App and backend systems were conducted in October 2015 and January 2017.

Vulnerabilities, and even non-input fields could be manipulated by the Mobile App's call to the API and that this should be remedied.

24 Based on the findings and recommendations in the 2015 Penetration Test Report, the Organisation ought to have been more diligent in performing a thorough assessment of the security posture of the API and the server. The Organisation should have examined all other functions to determine whether they could be exploited by changing the input parameters and implement the relevant fixes, but it had failed to do so.

25 For the reasons above, the Commissioner finds that the Organisation is in breach of section 24 of the PDPA as it failed to make reasonable security arrangements with respect to the said API to protect the personal data in its possession and within its control.

26 The Organisation submitted representations after a preliminary grounds of decision was issued and raised four points. First, the Organisation asserted that it was reasonable that any request parameters sent by the Mobile App during a login session was treated as valid without having to re-validate the request parameters during the session, given that the user was required to be legitimately authenticated via one of the three login methods. This does not address the Direct Object Reference Vulnerabilities which could be exploited by a third party. Paragraphs 15 to 25 above, deal with this point.

27 Secondly, the Organisation asserted that not all of its 330,000 customers' data was put at risk of disclosure as the informant would have had to use the correct combination of the mobile number of the customer, the customer's billing account number, billing account ID and billing cycle date in order to generate a bill specific to that customer or a correct mobile phone number to generate the

relevant subscription information. The Organisation thus asserts that the decision should be narrowed to only the 4 accounts that were successfully accessed. The manner in which the informant was able to access the records of the said 4 accounts is set out above at paragraphs 7(a) and 7(b). While the informant only accessed 4 accounts, the informant or someone with similar skillset and access to the same resources could potentially have access to the personal data of all 330,000 subscribers who were using the Mobile App during the material time of the Incident. In the circumstances, it is correct that the full size of the database was one of the factors taken into consideration in assessing the financial penalty quantum.

28 Thirdly, in reference to paragraph 19 above, the Organisation asserted that the technical expertise required by someone to exploit the Direct Object Reference Vulnerability was underestimated in this Decision. For the avoidance of doubt, it is agreed that some level of technical expertise would have been required for someone to exploit the Direct Object Reference Vulnerability. While this level of technical expertise is not uncommon, what cannot be ignored is that the vulnerability is well known and the requisite knowledge, tools and software to exploit the Direct Object Reference Vulnerability can be acquired online. This increases the likelihood that someone with the wrong motivation could have exploited the vulnerability.

29 Finally, the Organisation also restates that the Direct Object Reference Vulnerability was not detected in the security penetration tests. This is dealt with at paragraph 21 above.

30 In the circumstances, the Commissioner decided to maintain his finding that the Organisation was in contravention of section 24 of the PDPA. Nevertheless, the Commissioner has decided to impose a reduced financial

penalty quantum as set out at paragraph 32 below, given that the exploitation of the vulnerability requires some level of technical expertise.

The Commissioner's Directions

31 Given the Commissioner's findings that the Organisation is in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to issue such directions as it deems fit to ensure compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1 million.

32 Having considered all the relevant factors in this case, the Commissioner hereby directs the Organisation to pay a financial penalty of $25,000 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[6] in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full. The Commissioner has not set out any further directions given the remediation measures that the Organisation has already put in place.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION

[6] Cap 322, R5, 2014 Rev Ed.