Funding Societies Pte. Ltd.

[2018] SGPDPC 29

Tan Kiat How, Commissioner — Case No DP-1708-B1035

Data Protection – Protection obligation – Disclosure of personal data – Insufficient security arrangements

Data Protection – Personal data – Disclosure of financial information – Stronger controls needed to protect sensitive personal data

13 December 2018.

Background

1 On 14 August 2017, the Personal Data Protection Commission (the "**Commission**") received an email notification from the Organisation. The Organisation is the operator of an online financing platform that connects borrowers and investors (the "**Website**"). Individuals who used the Website would have to register for an account, either as an "Investor" or a "Borrower" (collectively, "**Members**"). Each Member was given a unique identifier, which was generated sequentially (the "**MemberID**").

2 In its email notification, the Organisation informed the Commission that one of its Members, [Redacted] (Replaced with "**Mr J**"), had emailed them on 25 July 2017 to inform that he had found a vulnerability with the Website. To illustrate this, Mr J showed the Organisation the personal details of two other Members that he had extracted from the Website (the "**data breach**"). The

Organisation took immediate action to rectify the vulnerability and was able to do so by 26 July 2017.

3 After receipt of the email notification from the Organisation, the Commission proceeded to investigate into an alleged breach of the Personal Data Protection Act 2012 ("**PDPA**").

Material Facts

The Website's vulnerability

4 On 19 June 2017, the Organisation rolled out new system components for the Website. This update gave rise to a vulnerability in the Website's security system, the details of which are summarised below.

5 When a Member successfully logged into the Website using his username and password, his browser received an *authentication* token from the Website's server.[1] This token contained the user's MemberID and granted the user access to the Website. Simultaneously, his browser also received an *authorisation* token, containing the same MemberID. The authorisation token controlled the functions and type of data that the particular user could access. Operating together, the two valid tokens (ie authentication and authorisation tokens, which shared the same MemberID) granted the logged-in user access to the Website's functions and data from his own Member account.

---

[1] A token is part of the request command from the browser to the Website. Token based authentication works by ensuring that each request to a server is accompanied by a signed token which the server verifies for authenticity and only then responds to the request.

6 However, the Organisation's in-house Website developers did not programme the Website to require both tokens to contain the same MemberID. When a logged-in user carried out a browsing activity on the Website, the security system only verified that the user's authentication token was valid, and thereafter granted data access based on the MemberID in the authorisation token, without ensuring that the MemberIDs in both tokens were identical.

7 As a result, a Member who had successfully logged into the Website (under an authentication token which carried his MemberID) could browse another Member's data by changing the MemberID in the authorisation token. The Organisation suspects that this is how Mr J had gained unauthorised access.

8 The investigations revealed that the Organisation became aware of this vulnerability on 7 July 2017, 18 days before the data breach occurred. The vulnerability was detected by a member of the Organisation's engineering team. Upon discovery, the Organisation initially planned to roll out a quick-fix within a week, and thereafter to have a complete fix within a month.

9 According to the Organisation, a quick-fix was rolled out on 11 July 2017, but had to be retracted on the same day as it caused the Website's mobile applications to crash. The Organisation then worked on finding a fix that would close out the vulnerability without causing the Website's mobile applications to crash.

10 On 20 July 2017, the Organisation rolled out a partial-fix for about 25% of their "endpoints".[2] They did not roll out the entire fix as they wanted to

---

[2] The Organisation explained that the "endpoint" referred to a function defined on the gateway which had a HTTP URL. The Commission understands the "endpoint" in this case to refer to the server which controlled access to their data.

"minimise the chances of inducing a negative effect" on their system. Although there was no evidence that this partial-fix had solved the vulnerability, the Organisation claimed that if Mr J had attempted access through one of the fixed endpoints, he would have been denied access to the data.

11 Before the Organisation could roll out a complete fix for the vulnerability, Mr J informed them of the data breach on 25 July 2017. The Organisation escalated the matter as top priority and rolled out the complete fix within 24 hours of Mr J's report.

12 In total, the vulnerability lasted for about 37 days.

The affected Personal Data

13 Mr J had accessed and extracted the personal data of two Members. In particular, the personal data that had been extracted included the Members' Customer ID, name, NRIC number, and residential address.

14 While there was no further evidence of unauthorised access, the investigations revealed that the personal data of all the Organisation's existing Members were also at risk of disclosure. At the time of the data breach, the personal data collected and held by the Organisation numbered in the thousands. The personal data that was at risk of disclosure included a Member's Customer ID, NRIC number, account username, first and last name, telephone number, marital status, spouse's name, residential address, bank account details (for investors), subscription agreement (for investors), crowdfunding settings (for investors), suitability assessment settings (for investors), wallet account balance (for investors), and company details (for borrowers).

15 Notably, an unauthorised user would have been able to pretend to be another user by using the other user's MemberID as the authorisation token to perform certain functions in respect of the other user's account. In particular, this included:

(a) Using the Investor's account to contact prospective Borrowers;

(b) Updating a Member's personal details (subject to actual verification of the details);

(c) Providing feedback to the Organisation on behalf of the Member;

(d) Changing the Member's email address which was used to subscribe to the Organisation's newsletter; and

(e) Altering the auto-investment settings of an Investor's account.

16 With regard to paragraph 15(e), it was revealed that an unauthorised user would have been able to delete the Member's auto-investment settings, or to alter the parameters for the Member's auto-investment settings. Such an alteration of the auto-investment parameters may have caused the Member to make an investment which he had not initially intended or to fail to make an investment which he may have wanted.

17 There was no evidence that Mr J, or any other person, had performed any of the unauthorised functions in paragraph 15.

The Organisation's Remedial Measures

18 Following the incident, the Organisation immediately requested Mr J to delete the data which he had accessed as a results of the vulnerability. Although the Organisation had requested written confirmation for this, they were only able to obtain verbal confirmation from Mr J that the data had been deleted.

19 The Organisation also took the following remedial actions to resolve the Website's vulnerability:

(a) Introduce a more robust logging system to log all unauthorised access to user account data;

(b) Forming an internal quality assurance team ("**QA team**");

(c) Implementing documentation requirements which required the QA team to create and maintain details of test cases and test results;

(d) Applying secure connection technologies or protocols, such as Transport Layer Security (TLS) protocol, to all websites and web applications handling personal data;

(e) Storing documents containing personal data on Amazon Web Service's Simple Storage Service (S3), which allows the storage of data in private buckets that require credential keys which are provided only when requests are authenticated; and

(f) Developing and implementing policies and procedures to manage future rollouts of new system components.

FINDINGS AND BASIS FOR DETERMINATION

20 The key issue to be determined is whether the Organisation had complied with its data protection obligations under section 24 of the PDPA.

21 Section 24 of the PDPA requires an organisation to protect the 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 (the "**Protection Obligation**").

22 As to the standard of reasonable security arrangements, the Commissioner has clarified in *Re Aviva Ltd* [2017] SGPDPC 14 that organisations must protect personal information by implementing security safeguards appropriate to the sensitivity of the information and that "more sensitive information should be safeguarded by a higher level of protection".[3]

23 In the present case, the Organisation possessed a wide range of personal data of their Members, including financial information such as bank account details and wallet account balance. The Commissioner considers the financial information of an individual to be "sensitive personal data".[4] It is also noteworthy that such sensitive personal data was readily accessible on the Website via a logged-in account.

24 Having considered the material facts, the Commissioner found that the Organisation did not have reasonable security arrangements in place to prevent the unauthorised access, use and disclosure of personal data in its possession.

25 First, the Organisation did not have adequate security arrangements on their Website to ensure that Members could only access their own information and perform functions on their own accounts. The decoupling of authentication and authorisation into two separate tokens was a deliberate design decision on

---

[3] *Aviva Ltd* [2017] SGPDPC 14 at paragraph [19].

[4] *Credit Counselling Singapore* [2017] SGPDPC 18 at paragraph [15].

the Organisation's part so as to "enable stateless API development". However, the Website should have been equipped with a security measure to ensure that the two tokens carried the same MemberID before granting access to data.

26 In the Commissioner's view, implementing such a security measure was a necessary step that the Organisation should have taken after decoupling the tokens. The lack of such security measures was a fundamental mistake on the Organisation's part, and left a glaring vulnerability in the Website. Indeed, this vulnerability was so obvious that the Organisation's own engineer had discovered it in the course of his routine work.

27 Second, the Organisation did not adequately test the security of their Website. The Organisation claimed that they had conducted testing prior to the rollout of the new Website components, but were unable to provide documentation of such testing. In any case, the Organisation explained that the tests focused on functionality and load testing of the Website, but not on the security and protection mechanisms. In this regard, it was clear to the Commissioner that the Organisation had failed to conduct the necessary security tests on its Website. Consequently, the Organisation failed to identify the vulnerability during its testing stage.

28 Third, the vulnerability in the Website could be exploited with relative ease. A Member who had some understanding of web technology would have been able to change the MemberID on the authorisation token, thereby granting him access to another Member's profile. While making such a change was not as simple as manipulating the URL, the Commissioner noted that the tools necessary to make such changes were not sophisticated and were readily available online. Crucially, the fact that MemberIDs were generated in a

sequential order made it even easier for Members to guess other Members' MemberIDs.

29 Fourth, the Organisation failed to appreciate the degree of risk that the vulnerability posed to the personal data in their possession. This was evident in their treatment of the vulnerability after their engineer discovered the breach. They had resolved to fix the vulnerability on 7 July 2018 but did not actually prioritise this until the breach occurred on 25 July 2018. The Organisation's explanation that it had only rolled out 25% of the partial-fixes to minimise the impact on their system revealed that they were uncertain about the effectiveness and compatibility of their partial-fix. It also reflected that they had not taken the vulnerability seriously, and that they were in no rush to fix the vulnerability so long as their business remained operational.

30 As such, the Commissioner finds that the Organisation had failed to make reasonable security arrangements to protect the personal data in its possession and within its control. The Organisation is, therefore, in breach of section 24 of the PDPA.

Representations by the Organisation

31 The Organisation made representations following the issuance of a preliminary Decision to the Organisation. The representations did not substantively address the Commissioner's decision to find the Organisation in breach of its obligations under the PDPA but were in the nature of a request to consider mitigating circumstances. The Commissioner has considered the representations and has decided to maintain the directions in the preliminary Decision.

32 The representations made by the Organisation are summarised below:

(a) The Organisation is a relatively young enterprise that has been in operation for less than 4 years and while, it takes "all reasonable efforts to ensure that any security issues and deficiencies are identified, handled and remedied on a proactive basis", there are some issues or deficiencies that it reactively dealt with. In the present case, once the incident was known, the Organisation notified PDPC of its breach voluntarily; and

expanded reasonable efforts to remediate the incident promptly;

(b) The Organisation continued to assess the data breach incident after its remediation efforts to develop long term procedures to prevent similar occurrences in the future;

(c) The Organisation had in place a framework of security arrangements, such as a risk management framework, an information security policy and training and audits of its policies and procedures;

(d) Only the data of two individuals were actually disclosed in the incident and no actual loss or damage was suffered; the actual compromised data did not include any financial information. Furthermore, the Organisation received verbal confirmation from the individual who discovered the flaw in the system that he had deleted the personal data of the two individuals that he extracted.

33 The Commissioner did not consider being a young organisation to be a mitigating factor. Neither should the fact that the Organisation continuously assessed its compliance with the obligations set out in the PDPA and that it had the necessary frameworks in place mitigatory as these were the standard of

conduct expected for compliance. These are not activities or measures which go beyond the standard of protection required by the PDPA and as such is not a mitigating factor.

34 With respect to point (d) above, this had already been taken into consideration when the Commissioner decided on the financial penalty.

ENFORCEMENT ACTION BY PERSONAL DATA PROTECTION COMMISSION

35 Given that the Commissioner has found the Organisation in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding $1 million as the Commissioner thinks fit.

36 In assessing the breach and determining the directions to be imposed on the Organisation, the Commissioner took into account the following factors:

Aggravating Factors

(a) The personal data of more than 4,000 individuals were at risk of unauthorised access, use and disclosure;

(b) The personal data which was at risk included financial information and was sensitive in nature;

(c) An unauthorised user would have been able to alter a Member's investment parameters, which could have led to actual financial losses;

(d) The Organisation was unable to confirm that Mr J had only accessed and extracted the personal data of two Members;[5]

Mitigating Factors

(e) The Organisation did not make reasonable efforts to rectify the vulnerability despite being made aware of it early;

(f) The Organisation voluntarily notified the PDPC of the breach;

(g) The Organisation was generally co-operative and forthcoming in providing timely responses to the Commission during the investigation; and

(h) The Organisation took prompt corrective action to resolve the vulnerability after being alerted to the data breach incident, as well as other remedial measures to improve its Website security.

---

5 The Organisation stated that their "system logging did not capture information required to show when [Mr J] was accessing the other user's account data". It was possible that Mr J had accessed and extracted the account data of countless other Members.

37 Having carefully considered all the relevant factors of the case, the Commissioner has decided to impose a financial penalty of $30,000 on the Organisation. This financial penalty is to be paid within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
DEPUTY COMMISSIONER
[FOR COMMISSIONER] FOR PERSONAL DATA PROTECTION