DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1409-A145

FEI FAH MEDICAL MANUFACTURING PTE. LTD.
(UEN No. 199800455H)

…Respondent

Decision Citation: [2016] SGPDPC 3

GROUNDS OF DECISION

20 April 2016

Background

1. Fei Fah Medical Manufacturing Pte. Ltd. (UEN 199800455H) ("**Fei Fah Medical**") is a locally registered company specialising in the development and manufacture of healthcare and beauty products.

The Ripple Website

2. Fei Fah Medical operates a website under the name Ripple Tea Company at www.ripple.com.sg ("**Site**").

3. The Site consists of both publicly accessible pages, and a members' portal (which is accessible only by individuals who had signed up with Fei Fah Medical under a membership scheme called Ripple Club, upon logging into the portal with their respective user identifications ("**IDs**") and passwords).

Data Leak Incident

4. On 29 September 2014, the Personal Data Protection Commission ("**Commission**") was informed that information of users of the Site had been posted on http://pastebin.com ("**Pastebin**"), a website which allows members of the public to post and share text online publicly (the "**Data Leak**").

5. The relevant information was ostensibly uploaded onto the Pastebin website by a Pastebin user with the username "KAMI_HAXOR", in the form of a post in plain text that could be publicly viewed by any visitor to the Pastebin website.

6. The post was undated and captioned "*Ripple Tea Company Singapore 900+ Users emails+passes+Names+mobile Numbers With Subscribers Emails Leaked By KaMi HaXor*".

7. The post contained a list of data, which were numbered from 1 to 2,981, ostensibly to indicate that there were 2,981 entries in it. The data in the post appeared to be have been sorted into the following three categories:

   (a) Email addresses – there were 1114 entries of email addresses. The email addresses were unaccompanied by other data or identifiers. 219 of the entries contained "*.sg*" domain names;

   (b) User ID and encrypted passwords to Ripple Club accounts – there were 876 entries of user IDs and passwords, which had been encrypted using an MD5 message-digest algorithm, a commonly used cryptographic hash function producing a 128-bit (16-byte) hash value; and

   (c) Telephone numbers – there were 836 entries of telephone numbers containing between seven and ten digits. It was unclear whether the telephone numbers were Singapore or Hong Kong telephone numbers as the format of telephone numbers used by the countries is similar.

8. In light of the information received, the Commission commenced an investigation under section 50 of the Personal Data Protection Act 2012 (No. 26 of 2012) (the "**Act**") to ascertain whether there had been a breach by Fei Fah Medical of its obligations under the Act.

Nature of the Data Leak Incident

9. In its responses to the Commission, Fei Fah Medical confirmed that the data in the list were those of prospective customers and general enquirers to its Ripple brand products.

10. Fei Fah Medical further confirmed that the data was collected via its Site and stored in a database based in Hong Kong. Fei Fah Medical had outsourced all its web development and hosting functions to its Hong Kong-based data intermediary, IT Factory. IT Factory had in turn engaged HKNet Company Limited, also based in Hong Kong, to provide the actual hosting services for the database.

11. Fei Fah Medical indicated that it had no knowledge of the Data Leak prior to receiving the Commission's Notice dated 1 October 2014. However, after being alerted to the Data Leak, it sent email notifications to all affected individuals, informing them that there had been hacking activity on the Site and that their personal data may have been compromised.

12. Fei Fah Medical also took steps to instruct IT Factory to remove all data collecting functions from its Site. However, as these instructions failed to be carried out by IT Factory, new data continued to be collected via the Site till 30 July 2015 (almost ten months after Fei Fah Medical was first notified about the Data Leak), when the Commission alerted Fei Fah Medical to the fact that the Site still retained its data collecting functions.

13. Fei Fah Medical was unable to ascertain how the Data Leak could have occurred and did not appear to be familiar with the security measures which were used on the Site at the material time: In fact, in its responses to the Commission, Fei Fah Medical simply stated the cause of the Data Leak to be "unknown" and was unable to provide any logs or files capturing the intrusion to its data system.

14. Fei Fah Medical also appeared to be uncertain about which individuals or organisation had access to the leaked data. Although Fei Fah Medical initially stated that the leaked data was only accessible by "the actual host" HKNet Company Limited, it later clarified that the data was also accessible at the material time by its own backend administration staff (i.e. those who administered the database), and by using the staff ID of one of its directors, [Redacted] (Replaced with Mr L). Additionally, it admitted that it would have been possible for a hacker to access the database to extract the data by seeding "some program in the server".

15. Overall, Fei Fah Medical was unable to explain how the Data Leak occurred. It was also unable to explain or provide sufficient information on the security measures implemented on either the Site or database at the material time.

16. In relation to the number of individuals affected by the Data Leak, the Commission notes that the title of the post indicates that the data of approximately 900 users had been disclosed in the data list. Although Fei Fah Medical claimed that not all the information in the data list was accurate, it did not dispute the number of users who were affected by the Data Leak.

17. Having reviewed the relevant facts and circumstances, including the written responses to the NTPs[1] submitted by Fei Fah Medical, the Commission sets out below its findings and assessment in relation to the Data Leak.

THE COMMISSION'S FINDINGS AND ASSESSMENT

Personal Data Leaked

18. As noted above, there were three categories of data found in the post at the Pastebin website. Fei Fah Medical acknowledged in its representations to the Commission that the data in the post were those of prospective customers and general enquirers to its Ripple brand products. Fei Fah Medical also acknowledged that personal data of Ripple Club members was stored in its database, which could be retrieved with the appropriate user ID and password.

19. Although the passwords were encoded, they had been encoded using an MD5 message-digest algorithm, a commonly used cryptographic hash function, which could be easily attacked with password tables by any motivated individual.

20. Further, given that anyone who had obtained a valid user ID and password combination would be able to log in to the Site to retrieve personal details

relating to the respective Ripple Club member, it is apparent that a valid user ID and password combination would be able to identify an individual Ripple Club member. Accordingly, the Commission is of the view that the user IDs and passwords that were leaked would fall within the definition of "personal data" in the Act.[2]

21. In addition, several of the telephone numbers disclosed in the data list appeared to be personal mobile telephone numbers, which would, by themselves, be able to lead to the identification of the individuals owning the numbers. Similarly, several of the email addresses display, what seems to be, the full names of the respective owners of the email addresses, and appear capable of identifying them. Those telephone numbers and email addresses thereby constitute "personal data" under the Act.[3]

Personal Data under the Possession and Control of Fei Fah Medical

22. Fei Fah Medical confirmed the fact that the Site was fully owned and administered by it at all material times. The personal data of Fei Fah Medical's Singaporean users were also generally collected via the Site from Singapore.

23. For completeness, the Commission notes Fei Fah Medical's statements that:

(a) IT Factory, as Fei Fah Medical's website vendor, was engaged to supply and design the website and to provide maintenance upon request; and

(b) the contents collected via the Site were stored in a database hosted at the premises of HKNet Company Limited, a data hosting service provider, on a dedicated server.

24. It is apparent from the information provided by Fei Fah Medical that IT Factory and HKNet Company Limited, as Fei Fah Medical's vendors, undertook these functions on behalf of Fei Fah Medical.

25. Although Fei Fah Medical initially stated that the leaked data was only accessible by HKNet Company Limited, it subsequently clarified that the data was also accessible at the material time by its backend administration staff (i.e. those who administered the database), and by one of its directors, Mr L. In fact, Fei Fah Medical remained in control of the personal data stored in the database hosted by HKNet Company Limited at all material times, as evidenced by Fei Fah Medical's instructions to IT Factory to delete all the personal data subsequent to the Data Leak.

26. Accordingly, the Commission is satisfied that, at all material times, the relevant personal data of users of the Site and whose security was compromised as a result of the Data Leak, was in the possession and/or under the control of Fei Fah Medical.

Adequacy of Security Arrangements

27. Fei Fah Medical, being an organisation which had its Site users' personal data under its possession and/or control, is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").[4]

28. However, Fei Fah Medical was unable to provide any information about the security arrangements that it had put in place to protect either the Site or the server where the database of personal data collected was hosted.

29. Although Fei Fah Medical claimed that it had set up some firewalls within the administration control panel, it was neither able to provide details as to the nature of these firewalls nor any evidence as to their existence in its responses to the NTPs issued by the Commission.

30. In the Commission's view, the facts demonstrate that, prior to the Data Leak, Fei Fah Medical had made little effort to inquire into and/or ensure the security of personal data stored on the Site. Fei Fah Medical appeared to have little knowledge as to whether there were security measures implemented on its Site or the server where the database of personal data collected was hosted.

31. In light of the foregoing, the Commission is of the view that Fei Fah Medical has failed to make reasonable security arrangements in respect of personal data relating to users of its Site, as required under the Protection Obligation.

THE COMMISSION'S DIRECTIONS

32. At the time of this decision, the list of data appears to have been removed from the Pastebin website.

33. In determining the directions to be given to Fei Fah Medical, the Commission has given due consideration to all the relevant factors, including the following:

    (a) Fei Fah Medical had been neither cooperative nor forthcoming in its responses to the NTPs issued by the Commission as part of its investigations. In this regard, the Commission notes that Fei Fah Medical had provided incomplete responses to the first and second NTPs issued by the Commission, and initially ignored the third NTP issued by the Commission. Fei Fah Medical also took between three weeks to a month to respond to each NTP and its responses were not forthcoming; and

    (b) although Fei Fah Medical took steps to instruct its Hong Kong-based data intermediary IT Factory to implement remedial actions to address the Data Leak following its discovery on 1 October 2014, it did not ensure that its instructions were carried out by its data intermediary. The data intermediary only implemented remedial actions to address the Data Leak on 30 July 2015, more than ten months after Fei Fah Medical first discovered the Data Leak. This undue delay in

implementing the remedial actions suggests a continuing insouciance by Fei Fah Medical with respect to its obligation to make reasonable security arrangements to keep personal data in its possession or under its control protected.

34. Pursuant to section 29(2), and having completed its investigation and assessment of this matter, the Commission is satisfied that Fei Fah Medical has been in breach of the Protection Obligation under section 24 of the PDPA.[5]

35. The Commission notes from the representations submitted by Fei Fah Medical's lawyers on its behalf to the Commission that it intends to shut down the Site and replace it with a newly constructed website within 4 months. Having carefully considered all the relevant factors of this case, the Commission hereby directs Fei Fah Medical to do the following:

(a) Fei Fah Medical shall within 120 days from the date of the Commission's direction:

(i) implement a new website to replace the Site;

(ii) conduct a web application vulnerability scan of the new website; and

(iii) patch all vulnerabilities identified by such scan;

(b) Fei Fah Medical shall, in addition, submit to the Commission by no later than 14 days after patching all vulnerabilities identified by the abovementioned vulnerability scan, a written update providing details on:

(i) the results of the vulnerability scan; and

(ii) the measures that were taken by Fei Fah Medical to patch all vulnerabilities identified by the vulnerability scan; and

(c) Fei Fah Medical shall pay a financial penalty of S$5,000.00 within 30 days from the date of the Commission's direction, failing which interest, at the rate specified in the Rules of Court in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

36. The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA and with the Commission's directions.

LEONG KENG THAI
CHAIRMAN
PERSONAL DATA PROTECTION COMMISSION

[1] Notice to Require Production of Documents and Information under the Ninth Schedule to the Personal Data Protection Act 2012.
[2] Section 2 of the Personal Data Protection Act 2012.
[3] Section 2 of the Personal Data Protection Act 2012.
[4] Section 24 of the Personal Data Protection Act 2012.
[5] The Personal Data Protection Act 2012.