**DECISION OF THE PERSONAL DATA PROTECTION COMMISSION**

**Case Number: DP-1512-A612**

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

**And**

**Orchard Turn Developments Pte. Ltd.**

**... Organisation**

**Decision Citation: [2017] SGPDPC 12**

**GROUNDS OF DECISION**

6 July 2017

## A. BACKGROUND

1. In this case, the Complainant received two unauthorised emails, purportedly sent by the Organisation promoting "free" ION+ Reward points. Investigations discovered that an unknown perpetrator had gained unauthorised access to a server that held personal data of the Organisation's members. The perpetrator then used an application on the compromised server to send the unauthorised emails to the Organisation's members using their personal data that was held in the server. This data breach incident raised the question of whether the Organisation had met its Protection Obligation under the Personal Data Protection Act 2012 ("**PDPA**") to make reasonable security arrangements to sufficiently protect personal data held on the server.

2. The following sets out the Commission's findings following its investigations into the matter.

## B. MATERIAL FACTS AND DOCUMENTS

3. The Organisation is the property manager of ION Orchard, a retail mall in Singapore. The Organisation runs the ION+ Rewards Loyalty Programme ("**ION's Loyalty Programme**"), which awards its members points based on their purchases made at the mall. Super e-Management Limited ("**Super-E**"), a

Hong Kong-based Information Technology ("**IT**") service provider, manages the IT system for ION's Loyalty Programme.

The System Setup

4. ION's Loyalty Programme runs on the Loyalty Management System ("**LMS**") which comprises several interconnected servers. Only two servers are relevant to the Commission's investigation: the (i) Web and Electronic Direct Mailer server ("**EDM server**") and (ii) LMS & Reporting Server ("**LMS server**"). The LMS server was used to store the database of members' personal data, while the EDM server was used to send out emails to members of ION's Loyalty Programme who had subscribed to receive updates from ION Orchard.

5. For the purpose of sending these email updates to its subscribers, the Organisation would transfer a subscriber list containing personal data of the Organisation's subscribers on the LMS server to the EDM server every day. This transfer of the subscriber list from the LMS server to the EDM server was an automated process. The Organisation would then send these emails through a web application hosted on the EDM server ("**EDM Application**"), which was configured to allow access to users with an administrative account ("**admin account**"). After the Organisation had sent out the emails, the personal data of the subscribers were not purged but were instead retained on the EDM server. The personal data set that was stored on the EDM server comprised a subscriber's name, email address, birthdate, and membership registration date.

The Data Breach Incident

6. On 26 December 2015, an unknown perpetrator gained unauthorised access to the EDM Application using valid admin account credentials to access the subscriber list. The perpetrator then crafted unauthorised emails, which looked like they were genuine emails from the Organisation, promoting "free" ION+ Reward points (the "**Phishing Emails**") to the subscribers; before proceeding to send these Phising Emails out to 24,913 subscribers.

7. The Phishing Emails contained a link (http://fastlnks.com/7LIW) which directed a subscriber to an online advertisement website. The subscriber would be prompted to select one of the options on the website to obtain the bogus ION+ Reward points. If the subscriber selected any of the options, the subscriber would be directed to more advertisement pages which may request for the subscriber's personal data, such as the subscriber's mobile phone number or email address.

8. Subsequently, Super-E received an alert from the EDM server and discovered that an Internet Protocol address (IP address) from Egypt had successfully

logged into the system, and had sent out the Phishing Emails to the Organisation's subscribers. After discovery of the data breach, Super-E disabled the EDM server to prevent further dispatches of Phishing Emails to the Organisation's subscribers. On 27 and 29 December 2015, the Organisation sent emails to the affected subscribers informing them of the Phishing Emails that had been sent.

The KPMG Reports

9. The Organisation engaged KPMG Services Pte. Ltd. ("**KPMG**") to conduct an investigation into the data breach incident. KPMG found that the cause of the incident appeared to be "*an unauthorised access using 'admin' credentials via the EDM application*".

10. In addition, KPMG found several issues with the security posture of the EDM server. For example, KPMG found that the operating system of the EDM server was not patched or hardened, thus exposing the EDM server to potential exploitation. Additionally, KPMG conducted a vulnerability check which revealed that the EDM Application had 24 known vulnerabilities that could be exploited.

The Commission's Investigations into Super-E

11. Based on the Commission's investigations into the matter, the Commission understands that Super-E was involved in the management of the IT systems for the ION Loyalty Programme at the time of the data breach incident, and may therefore share some responsibility with ION for the protection of the personal data of the Organisation's subscribers. As Super-E is located in Hong Kong Special Administrative Region of the People's Republic of China, the Commission would pursue available options for assistance in this aspect of the investigations with the relevant foreign data protection authority.

12. In the meantime, the Commission has concluded its investigations into the Organisation's compliance with the PDPA, and has therefore proceeded to issue its grounds of decision focusing only on the Organisation's compliance with the PDPA.

## C. THE COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

Issue for Determination

13. The relevant issue for determination is whether the Organisation had put in place reasonable security arrangements to protect the personal data set in its possession or in its control, as required under section 24 of the PDPA.

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

*Increased Risk Due to the Organisation's System Setup*

14. As described above in paragraphs 4 to 5, the Organisation did not purge the personal data from the EDM server that were being transferred every day from the LMS server to the EDM server. After the emails had been sent out, the personal data of the subscribers were not deleted from the EDM server. The effect of this practice was that some of the personal data of the Organisation's members could be found in two different places – the LMS server and EDM server.

15. However, this retention of personal data on the EDM server was unnecessary. The LMS setup was designed in such a way that the primary database of customer data was stored on the LMS server, which had no direct connection to the Internet. The EDM server, on the other hand, was a separate server that had access to the Internet. Given that a subset of members' personal data was automatically transferred from the LMS server to the EDM server every day, only this subset of personal data was accessible from the Internet. Once the subscribers' personal data has been transferred to the EDM server, the process for each email blast was as follows: load the subset of personal data of subscribers, run the EDM Application, and use the EDM Application to blast the emails to the subscribers. There was no need to retain the personal data in the EDM server beyond this. The daily automatic transfer of data from the LMS server to the EDM server coupled with the retention of personal data on the EDM server created significant risks to the security of the personal data.

16. First, the daily automatic transfer effectively created a permanent store of personal data on the EDM server. This *de facto* permanent store of personal data had the effect of storing a duplicate or additional set of personal data on the EDM server (in addition to the LMS server). The EDM server was accessible from the Internet and its online accessibility made it more susceptible to online attacks and external threats, and it was therefore more likely to be compromised. By keeping a duplicate or additional set of personal data on the EDM server, the Organisation was placing unnecessary risks on the security of the personal data, should the EDM server be the subject of an attack or security compromise.

17. Second, the longer the personal data set was left on the EDM server, the more exposed it was to online attacks and external threats. If personal data is loaded onto the EDM server whenever there is – and only for the duration of – a scheduled email blast, and then promptly deleted, there would not have been a *de facto* permanent store of personal data on the EDM server. Prompt

deletion after each email blast would significantly narrow the window period for which the personal data on the EDM server is at risk of unauthorised access in the event that the EDM server is compromised. During investigations, the Commission discovered that the email blast is scheduled to take place approximately once a month. Further, in any given month, another email blast would also be made on an ad-hoc basis to certain categories of ION[PRIVI] members (a subset of all subscribers). The aforesaid email blast would therefore, be likely sent out via the EDM server more than once a month. It cannot be gainsaid that the risk had been significantly enlarged by keeping a *de facto* permanent store of personal data on the EDM server.

18. Third, the frequency of such transfers brings about an increased risk that personal data may be intercepted during transmission. In this regard, the daily automatic transfer of personal data from the LMS server to the EDM server, when compared with the much less frequent email blasts to subscribers (approximately on a monthly basis), exposes the personal data *in transit* to an unnecessarily enlarged risk of interception.

19. Additionally, by effectively establishing a permanent store of personal data on the EDM server (albeit a subset of subscribers who wished to received EDM emails), and given the attendant risks attached to it, there was a need for the Organisation to ensure that the extent of hardening the EDM server and security of the transmission route to the EDM server can meet the level of protection expected in order to comply with the PDPA. Once a server is known to hold or process personal data, the organisation has obligations to protect the personal data by ensuring that the personal data in transit to and from the server, and the personal data held in the server, are adequately protected.

20. In the final analysis, it was not prudent for the Organisation to keep a duplicate or additional set of personal data on the EDM server for a period longer than necessary. Accordingly, the Organisation's setup of the LMS in combination with its practice of retaining the personal data set on the EDM server was not in keeping with the reasonable security arrangements to be put in place.

21. In addressing the issues highlighted above, the Organisation may seek to include the standards for compliance with the Protection Obligation as part of its design specifications of the LMS. By adopting a data protection-by-design approach towards the enhancements to the LMS, it is conceivable that no more than modest enhancements may be necessary in order to meet the standards expected for compliance with the PDPA.

*Absence of Proper Policies or Practices to Safeguard Passwords*

22. The Commission also identified other issues concerning the security of the members' personal data. Foremost of them is the absence of policies or practices to safeguard the admin account passwords.

23. Although the Organisation was unable to establish the root cause of the data breach incident, what the Organisation, KPMG, and Super-E had found was that the perpetrator had gained unauthorised access to the EDM server in a single attempt. There was no evidence of hacking or that the perpetrator had deployed any brute force attacks. This suggests that it was likely that the perpetrator had managed to get hold of the valid admin account credentials to gain access to the EDM system.

24. In the course of investigations, the issue of whether the Organisation had put in place proper password management practices and policies came to the fore. The Commission found that the Organisation did not have any formal policy or practice for the management of the admin account passwords to the EDM server. In particular, the Organisation failed to implement any policy to prohibit the sharing of admin account credentials or to enforce periodic expiry and renewal of the same. In the following sections, we will look at the various authorities highlighting the importance of having proper password management policies and practices, and examine the organisation's failure to put proper password management policies and practices in this respect.

*(i) Foreign authorities highlight the importance of Password Management Policies*

25. The need for proper password management policies was highlighted in the report *Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner* ("**Joint Investigation**").[1] In that case, Avid Life Media Inc ("**ALM**"), a company incorporated in Canada that operates a number of dating websites including Ashley Madison, was the subject of a data breach incident in 2015. The hackers gained access to the details of 36 million ALM user accounts, which included personal information, and published the data online.

[1] *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner* (22 August 2016), PIPEDA Report of Findings #2016-005, online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/>.

26. In their joint report, the commissioners found that ALM had poor key and password management practices, given that it had made available on ALM's Google drive, the "shared secret" to its Virtual Private Network ("**VPN**"). This meant that "*anyone with access to any ALM employee's drive on any computer, anywhere, could have potentially discovered the shared secret*". The commissioners concluded that such practices constituted "*failures to take reasonable steps to implement appropriate security safeguards in the specific circumstances, given the volume and nature of the personal information held by ALM*".

27. That the need for proper password management policies forms an important component of the security arrangements to protect personal data is also found in the case of *Twitter, Inc*.[2]

28. In that case, the Federal Trade Commission ("**FTC**") found that Twitter, a social networking website, had failed to, amongst other things, enforce periodic changes of admin account passwords, e.g. by setting passwords to expire every 90 days. Additionally, Twitter also failed to establish or enforce policies sufficient to make admin account passwords hard to guess. Accordingly, Twitter was found to have failed to provide reasonable and appropriate security measures to protect personal data.

*(ii) Foreign authorities highlight the importance of regular Changing of Passwords and Prohibition Against Sharing of Credentials*

29. Data protection authorities are also of the view that good password management policies encompass the regular changing of admin account passwords and the prohibition against sharing admin account credentials amongst multiple users.

30. The abovementioned case of *Twitter, Inc.* also stands for the point that there needs to be periodic changes to the admin account passwords. The effect of implementing periodic changes is that there will be a shorter window period, and thus fewer opportunities, for someone to try to crack the admin account passwords of the system.

31. Additionally, there should not be a sharing of credentials amongst users. When credentials are shared among multiple users, it is difficult to ensure accountability as it is difficult to track the activity of each individual using the common set of credentials.

---

[2] *In the Matter of Twitter, Inc., a corporation* (2 March 2011), FTC 092-3093 (No. C-4316), online: FTC <https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation>.

32. In the case of *Reed Elsevier Inc. and Seisint, Inc.*,[3] the Organisations had collected and stored in their databases non-public and highly sensitive personal information about millions of consumers, including consumer identification information obtained from credit reporting agencies. Attackers exploited the Organisations' poor security practices to obtain the user credentials of legitimate consumers, and used these credentials to make thousands of unauthorised searches for consumer information in the Organisations' databases. The FTC found that the Organisations had failed to adequately protect personal data because it had, amongst other things, a practice of permitting the sharing of user credentials among a customer's multiple users. According to the FTC, this had the effect of reducing the likely detection of, and accountability for, unauthorised access to the databases.

33. In this regard, the Information Commissioner's Office ("**ICO**") in the UK has advised organisations to "*issue all staff with unique usernames and passwords for the network and systems containing personal data*", and "*do not allow users to share passwords with their colleagues*".[4] Likewise, the Office of the Data Protection Commissioner of Ireland has expressly stated in its Data Security Guidance that "*[s]hared credentials should never be permitted*" and that data controllers should "*ensure that users are made aware that their password / passphrase is unique to them and must not be disclosed to anyone else*".[5]

34. In sum, the data protection authorities have taken the position that password management policies, especially the regular changing of passwords and prohibition against the sharing of credentials, are an important and integral part of IT security arrangements.

*(iii) The Organisation Failed to Implement Proper Password Management Policies Required*

35. On the facts, the Organisation failed to put in place any formal policy or practice for the management of the admin account passwords to the EDM server. Additionally, in terms of the Organisation's handling of the admin account credentials, the Commission identified two main areas of concern as follows:

---

[3] *In the Matter of Reed Elsevier Inc. and Seisint, Inc., corporations* (1 August 2008), FTC 0523094 (No. C-4226), online: FTC <https://www.ftc.gov/enforcement/cases-proceedings/052-3094/reed-elsevier-inc-seisint-inc-matter>.

[4] U.K., Information Commissioner's Office, *Findings from ICO advisory visits to residential sales and lettings organisations* (2016), online: ICO <https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/1560562/outcomes-report-residential-sales-and-lettings.pdf> at page 7.

[5] Republic of Ireland, Office of the Data Protection Commissioner of Ireland*, Data Security Guidance*, online: DPC <https://www.dataprotection.ie/docs/Data-security-guidance/1091.htm>.

(a) first, the Organisation only created a single admin account, of which the admin account credentials were shared among four authorised users. All these four users were sent the same admin account credentials in a single email from Super-E dated 28 January 2015. This 'sharing' of the admin account credentials multiplied the risks of a data breach by making it more difficult to pinpoint which user had been the source of the likely leak of credentials that enabled the unauthorised access to take place. At the same time, the EDM server would not have been able to ascertain (and account for) which of the users (whether authorised or not) had accessed the system, since the username and password was the same for all; and

(b) second, the password of the admin account to access the EDM Application had not been changed since the roll out of the EDM Application, i.e. from November 2014 until the time of the data breach incident in December 2015. The implementation of an effective password expiry mechanism would have reduced the potential adverse impact of an unauthorised use of the admin account password.

36. Accordingly, given the lack of proper password management policies and practices, the Commission was of the view that the Organisation had failed to put in reasonable security arrangements to protect the members' personal data.

*Other Issues with the Organisation's Security Arrangements*

37. Apart from the issues with the password management policies of the EDM server, the Commission also found other notable issues as follows.

38. First, the Organisation failed to ensure regular patching of the EDM Application since its roll out in November 2014. The KPMG Reports highlighted that the EDM Application was exposed to 24 known vulnerabilities because it did not follow a regular patching cycle. The KPMG also noted that the EDM server appeared to have been patched in an ad-hoc manner once every two to four months. Patching is one of the common tasks that all system owners have to perform in order to keep its security measures current against external threats. The failure to patch the EDM Application regularly was a failure to protect the EDM Application against known system vulnerabilities.

39. Second, the Organisation did not conduct any vulnerability assessment to detect if there were any vulnerabilities in the system prior to its roll out. As explained in *The Cellar Door Pte Ltd and Global Interactive Works Pte Ltd* [2016] SGPDPC 22, this meant that there was no systematic way of identifying vulnerabilities, and addressing those vulnerabilities. This posed as a limitation to the Organisation's ability to determine the technical measures that were

required to ensure that the personal data of its members were adequately protected.

40. The Commission understands that after the data breach incident, the Organisation purged all the personal data residing on the EDM server and subsequently put in place a purge policy where the personal data set on the EDM server will be removed after a standard period of 14 days.

41. In view of all of the relevant facts and circumstances, the Commission finds that Organisation has not made reasonable security arrangements to protect personal data and is in breach of section 24 of the PDPA.

## D. THE COMMISSION'S DIRECTIONS

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

43. In assessing the breach and determining the directions to be imposed to the Organisation in this case, the Commission took into account the following factors:

(a) a large number of individuals (a total of 24,913 subscribers out of a potential 47,635 subscribers that could have been impacted by the data breach incident) had the unauthorised Phishing Emails sent to them;

(b) the Phishing Emails had exposed the recipients to further risks and other exploits, ie through the pop-up windows that were intended to induce the recipients to provide their personal data;

(c) the Organisation did not make reasonable efforts to put in place proper password management policies, and to ensure the security of the personal data set by reasonably anticipating, identifying and rectifying the technical security vulnerabilities (as mentioned at paragraphs 38 and 39 above) at an earlier stage;

(d) the Organisation was generally cooperative and forthcoming in providing timely responses to the Commission during the investigation; and

(e) the Organisation took prompt remedial action after being alerted to the data breach incident, as well as other corrective measures to improve its IT security.

44. Having carefully considered all the relevant factors of this case, the Commission hereby directs the Organisation to do the following:

(a) within 60 days from the date of the Commission's direction to:

(i) patch all the system vulnerabilities identified by KPMG Reports dated 8 March 2016 and 19 April 2016;

(ii) conduct a penetration test on the Internet-facing portion of the Loyalty Management System and rectify weaknesses that have been identified; and

(iii) implement a password management policy and conduct training for staff on password management best practices;

(b) by no later than 14 days after the above action at paragraph 444(a) has been carried out, the Organisation shall, in addition, submit to the Commission a written update providing details on (i) the results of the penetration test; (ii) the measures that were taken by the Organisation to patch all system vulnerabilities; and (iii) the password management policy and the training; and

(c) pay a financial penalty of S$15,000 within 30 days from the date of the Commission's direction, failing which, interest at the rate of 6% per annum shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

**YEONG ZEE KIN**
**DEPUTY COMMISSIONER**
**PERSONAL DATA PROTECTION COMMISSION**