PERSONAL DATA PROTECTION COMMISSION

Case No. DP-1905-B3936

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

And

Chan Brothers Travel Pte Ltd

SUMMARY OF THE DECISION

1. On 23 May 2019, the Personal Data Protection Commission (the "**Commission**") received a data breach notification from Chan Brothers Travel Pte Ltd (the "**Organisation**") and a complaint from a member of the public. Both were in relation to personal data being at risk of unauthorised access through the Organisation's website at http://chanbrotherstravelclub.force.com (the "**Website**") (the "**Incident**").

2. In March 2017, the Organisation purchased Community Cloud, a product of Salesforce.com Singapore Pte Ltd ("**Salesforce**"), to host the Website. The Organisation managed the Website internally. In August 2018, the Organisation engaged Aodigy Asia Pacific Pte Ltd ("**Aodigy**") as an outsource vendor to maintain and improve the Website.

3. The Website provided three online forms for enquiries and feedback. These were the "Enquiry Form", Feedback Form" and "Post-Tour Feedback Form" (collectively the "**Forms**"). The Forms collected the users' names, email addresses and mobile phone numbers.

4. In March 2018, there was a software update released by Salesforce for Community Cloud. This software update included an automated search engine optimisation feature (the "**SEO**"). As the Website's access configuration was set to "Public", the Forms automatically inherited the same setting for the purpose of the SEO feature. The result was that the personal data of an estimated 5,593 individuals collected by the Forms were indexed and cached, and made searchable, through online web search engines.

5. Organisations that employ IT systems or features are responsible for data security. Organisations must acquire knowledge of the security settings and be aware of security implications of software features of their IT system, and they must configure the security settings to enable effective protection of personal data stored in the IT system. This responsibility extends to new features introduced by subsequent software releases. Organisations that lack the IT knowledge to discharge this responsibility should engage qualified assistance.

6. The Organisation failed to consider the implication of the "Public" setting of the Website on the security of the data collected by the Forms. It also failed to understand the function and operation of the SEO feature. The combination of these acts of omission resulted in the security issues arising leaving the SEO feature enabled.

7. The Organisation claimed not to have received any notification from Salesforce of the SEO release. However, this is contradicted by the following. First, the notes of the software release was published on the website of Salesforce. Second, Aodigy had (in its role as vendor for another project) received information of the release. On balance, it is

therefore unlikely that Salesforce would have omitted to notify the Organisation about the software release. In any event, the software release was in March 2018 when the Organisation was still maintaining the Website internally. The responsibility to assess the security implications of the software release laid squarely on its shoulders during that 5-month period before Aodigy was engaged.

8. Further, there is some uncertainty over whether Aodigy was instructed to review the security configuration of the Website (including the new software features) as part of its maintenance services when it was engaged. The Organisation did not give clear instructions to Aodigy to assess the security configuration of the IT system as part of the maintenance services.

9. In the circumstances, the Deputy Commissioner for Personal Data Protection therefore found the Organisation in breach of section 24 of the Personal Data Protection Act 2012 and took into account the following factors in deciding to issue a Warning to the Organisation:

   a. The personal data at risk of disclosure was limited to names, email address and contact numbers, apart from an estimated 50 NRIC numbers.

   b. The Organisation voluntary notified the Commission of the Incident.

   c. Prompt co-operation in the course of the Commission's investigations.

10. No directions are required as the Organisation took immediate steps to prevent the recurrence of the Incident.