PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2102-B7854

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

And

Southaven Boutique Pte Ltd

Editorial note: An application for reconsideration was filed against the decision in *Re Southaven Boutique Ptd Ltd.* Pursuant to this application, the Deputy Commissioner has decided to reduce the financial penalty imposed on the Organisation from $5,000 to $2,000. As the application did not give rise to significant legal or factual issues, a separate decision on the application will not be published.

SUMMARY OF THE DECISION

1. On 5 February 2021, Southaven Boutique Pte Ltd (the "**Organisation**"), a brick-and-mortar retailer of clothes and accessories, informed the Personal Data Protection Commission (the "**Commission**") of a ransomware attack that occurred on or about 4 February 2021 (the "**Incident**"). A threat actor had gained access to the Organisation's Point-Of-Sale (the "**POS**") system server and encrypted the personal data of 4,709 customers. The personal data affected include names, addresses, email addresses, contact numbers and date of birth.

2. Investigations revealed that the Organisation did not implement adequate administrative and technical security arrangements. First, the Organisation failed to conduct or schedule any software updates, maintenance and/or security review before the Incident. Past decisions by the Commission had stressed the need for such security arrangements. The Organisation's operating system and anti-virus software, for example, were outdated and updated only after the Incident.

3. Second, the Organisation had failed to set out any data protection requirements or responsibilities with the POS vendor whom the Organisation had engaged to supply and install the POS, and relied on for system service issue. This meant that the Organisation did not in fact engage the POS vendor to provide the necessary maintenance support. As the Organisation continued to seek the POS vendor's assistance for any system service issue, it was also not entirely clear to the parties concerned whether the POS vendor remained responsible for ensuring that the POS system server was updated or patched. It should be reiterated that while an organisation may engage other third-party service providers to provide the

necessary technical assistance and support, an organisation's responsibility for complying with its statutory obligations under the PDPA may not be delegated.[1] Given the Organisation's omission to engage any maintenance support prior the Incident, the Organisation bore full responsibility for its failure to conduct or schedule the necessary software updates, patches and security reviews.

4. In the circumstances, the Organisation is found to have breached section 24 of the Personal Data Protection Act 2012 (the "**PDPA**").

5. After the preliminary decision was issued, the Organisation submitted representations requesting for a waiver of the financial penalty imposed. The Commission considered the representations made, and took into account first, the remediation efforts taken by the Organisation since the Incident, and its commitment to invest in a better and more secure IT system, and second, the adverse impact the COVID-19 pandemic had on the Organisation's business revenue. Nonetheless, as explained above, the onus remained on the Organisation to put in place adequate security measures such as regular IT system maintenance, patches and periodic security reviews.

.

6. Having considered all the circumstances in this case, the Deputy Commissioner directs that the Organisation pays a financial penalty of S$5,000 within 30 days from the date of the notice accompanying this decision, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

7. Finally, having considered the remedial actions taken by the Organisation, the Commission will not issue any directions under section 48I of the PDPA.

[1] See *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317 at [14] and [23].

The following is the provision of the Personal Data Protection Act 2012 cited in the above summary:

Protection of personal data

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.