PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2009-B6931

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

And

Webcada Pte Ltd

SUMMARY OF THE DECISION

1. On 4 September 2020, Webcada Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") that three of its database servers had been subjected to a ransomware attack on 29 August 2020 (the "**Incident**").

2. The personal data of 522,722 individuals were affected in the Incident. The datasets affected comprised of the individuals' names, phone numbers, dates of birth, addresses and order histories.

3. Following the Incident, the Organisation engaged an independent third-party consultant to investigate, review and assist in the implementation of additional data protection measures.

4. Investigations revealed that the ransomware had been uploaded onto the affected servers via the Intelligent Platform Management Interface ("**IPMI**"). The IPMI is a set of computer

interface specifications used for remote monitoring and management of servers. There was no evidence of data exfiltration, and all affected data was restored from available back-ups.

5. The Organisation took the following remedial measures after the Incident:

(a) IPMI was permanently disabled for all servers;

(b) The public IP address of all servers was removed and all remote management access to the servers was configured to allow only trusted IP addresses;

(c) End-point protection software with threat hunting capabilities was installed on all servers and computers within the Organisation; and

(d) A written data protection policy was developed and implemented to comply with the provisions of the Personal Data Protection Act 2012 (the "**PDPA**").

6. In its representations to the PDPC, the Organisation admitted to having breached the Accountability Obligation under section 12 and the Protection Obligation under section 24 of the PDPA, and requested for the matter to be dealt with in accordance with the PDPC's Expedited Decision Procedure.

Section 12 of the PDPA

7. First, the Organisation admitted it did not have a written data protection policy prior to the Incident. In this regard, it is important to reiterate that an organisation must document its data protection policies and practices in writing as they serve to increase awareness and

ensure accountability of the organisation's obligations under the PDPA. This requirement has been emphasized multiple times in previous decisions[1].

Section 24 of the PDPA

8. Second, the Organisation admitted that it did not configure its IPMI access settings correctly prior to the Incident. It enabled access to the IPMI from the public Internet when this was not necessary. Furthermore, in the monthly vulnerability scans carried out by the Organisation, it had omitted to scan the IPMI. Hence, it was not able to detect vulnerabilities in its IPMI, which were exploited to gain access to and upload the ransomware on the servers.

9. In the circumstances, the Organisation is found to have breached sections 12 and 24 of the PDPA.

10. After considering the factors listed at section 48J(6) of the PDPA and the circumstances of this case, including (i) the Organisation's upfront voluntary admission of liability which significantly reduced the time and resources required for investigations; and (ii) the Organisation's prompt remedial actions, the Organisation is given notice to pay a financial penalty of $25,000.

[1] See *Re Aviva Ltd* [2017] SGPDC 14 at [32]; *Re Singapore Taekwondo Federation* [2018] SGPDC 17 at [39] to [42]; *Re AgcDesign Pte Ltd* [2019] SGPDC 23 at [4] to [5]; *Re (1)Everlast Projects Pte Ltd (2)Everlast Industries (S) Pte Ltd (3) ELG Specialist Pte Ltd* [2020] SGPDC 20 at [8] to [9]

11. The Organisation must make payment of the financial penalty 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.

12. In view of the remedial actions taken by the Organisation, the Commission will not issue any directions under section 48I of the PDPA.