PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2102-B7884

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

And

Sendtech Pte. Ltd.

… *Organisation*

SUMMARY OF THE DECISION

1. On 13 February 2021, Sendtech Pte. Ltd. (the "**Organisation**") informed the Personal Data Protection Commission (the "**Commission**") of a data breach incident. There was an unauthorized access to the Organisation's Amazon Web Services ("**AWS**") account via an access key (the "**Incident**").

2. The Organisation became aware of the Incident on 10 February 2021 when its AWS account was shut down due to unusual account activity. The cause of Incident was a compromised AWS access key. This access key was created in 2015 when the Organisation was developing the backend of its server in its incipient stages. This AWS access key had not been rotated or changed since 2015. The Organisation suspected that the AWS could have been compromised through its former or current employees. First, all former developers had access to this key and some could still have the source code on

their computers. Second, as most of the employees are working from home, it is possible that the AWS access key was compromised if the employees had accessed internet through a public WiFi connection.

3. With this compromised AWS access key, the attacker gained admin privileges, created another admin account and queried the buckets storing personal data. As a result, the personal data of 64,196 customers and 3,401 contractors and the contractors' employees were accessed. There was no evidence of data exfiltration. For the customers, the personal data included the email address, contact number, home address and last four digits of the debit or credit card. For the contractors and their employees, the personal data included profile photo and copies of the NRIC or work permit (front and back).

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

   a. Rotated all access keys;
   b. Changed passwords for all servers;
   c. Enhanced its audit trail on AWS buckets to log all read and write operation at the object level;
   d. Checked and verified that its Github repositories was set to "Private";
   e. Engaged cybersecurity consultants to carry out assessment of its security setup and advise on improvements to the security measures; and
   f. Developed new cybersecurity policies and processes which specifically include measures for credentials management.

5. In its representations to the Commission, the Organisation admitted to having breached the Protection Obligation under section 24 of the Personal Data Protection Act (the "**PDPA**"), and requested for the matter to be dealt with in accordance with the Commission's Expedited Decision Procedure.

6. The Organisation admitted it did not have specific AWS policies for the assignment of roles to rotate credentials. There was also a lack of detailed steps to manage credentials access of outgoing staff. Hence, the credentials were not rotated or changed whenever there are staff movement.

7. In the circumstances, the Organisation is found to have breached section 24 of the PDPA.

8. On 23 June 2021, the Organisation was notified of the Commission's intention to impose a financial penalty of $10,000 based on the Commission's consideration of the factors listed under section 48J(6) of the PDPA, and the circumstances of this case, in particular (i) the Organisation's upfront voluntary admission of liability which significantly reduced the time and resources required for investigations; and (ii) the prompt remedial actions undertaken by the Organisation. The Organisation was invited to make representations. Having considered the Organisation's representations dated 25 June 2021 to reduce the financial penalty payable and to allow the Organisation to pay the financial penalty by way of an instalment plan the Deputy Commissioner hereby directs the Organisation to:

a. Pay a financial penalty of $9,000 in 12 instalments by the due dates as set out below, failing which the full outstanding amount shall become due and payable immediately and 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:

i. 1st instalment of $750 on 1 September 2021;

ii. 2nd instalment of $750 on 1 October 2021;

iii. 3rd instalment of $750 on 1 November 2021;

iv. 4th instalment of $750 on 1 December 2021;

v. 5th instalment of $750 on 1 January 2022;

vi. 6th instalment of $750 on 1 February 2022;

vii. 7th instalment of $750 on 1 March 2022;

viii. 8th instalment of $750 on 1 April 2022;

ix. 9th instalment of $750 on 1 May 2022;

x. 10th instalment of $750 on 1 June 2022;

xi. 11th instalment of $750 on 1 July 2022; and

xii. 12th instalment of $750 on 1 August 2022.

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