PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2102-B7878

In the matter of an investigation under section 50(1) of the

Personal Data Protection Act 2012

And

Singapore Telecommunication Limited

SUMMARY OF THE DECISION

1. On 10 February 2021, Singapore Telecommunication Limited (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a personal data breach that had occurred through the exploitation of zero-day vulnerabilities in a File Transfer Appliance ("**FTA**") provided by a third party system (the "**Incident**").

2. As a result of the Incident, 9,921 files containing personal data were exfiltrated. The personal data of 163,370 individuals which included their name, NRIC number, FIN, UIN, nationality, date of birth, address, email address, mobile number, photograph, staff, company pass or ID, bank account number, credit

card information (with expiry date), billing information, and vehicle number were affected.

3. The Organisation engaged an external cybersecurity company, FireEye Mandiant, to investigate the Incident. Its investigations found that the threat actors had exploited two (2) zero-day vulnerabilities of the FTA to gain unauthorised access to the FTA's MySQL database and subsequent file downloading.

4. Investigations revealed that the Organisation had a license to use the FTA with the FTA developer, Accellion Pte Ltd ("**Accellion**"). Accellion was the only party that had access to the proprietary source code to the FTA system. Accordingly, the discovery and rectification of the zero-day vulnerabilities within the FTA system fell within the sole responsibility and control of the developer. We are of the view that the Organisation could not have detected or prevented the incident as it had no control or visibility of the zero-day vulnerability of the FTA.

5. The Organisation had provided and made reasonable security arrangements to protect personal data in its possession and/or control in relation to the Incident. The Organisation maintained the practice of updating and patching the FTA within five (5) days of patch/update receipt.

6. Following the Incident, the Organisation took prompt and extensive remedial both to mitigate the effects of the Incident and enhance the robustness of its security measures. This included shutting down the FTA, conducting thorough

review of processes and file sharing protocols to enhance information security posture, and offering identity monitoring service to the affected individuals.

7. In view of the above, the Deputy Commissioner for Personal Data Protection is satisfied that the Organisation had met its Protection Obligation under section 24 of the PDPA and cannot be held liable for zero-day vulnerabilities on a third party system. No enforcement action therefore needs to be taken in relation to the Incident.

The following provision(s) of the Personal Data Protection Act 2012 had been 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.