PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2007-B6607

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

And

Singapore Telecommunications Limited

SUMMARY OF THE DECISION

1. On 15 July 2020, Singapore Telecommunications Limited (the "**Organisation**") informed the Personal Data Protection Commission of an incident which had occurred on or about 13 July 2020 (the "**Incident**"). In the Incident, a threat actor accessed the accounts of 17 of the Organisation's telecommunications service subscribers to request for issuance of new SIM cards, forwarding of voice calls and/or cessation of mobile services[1]. Once these were issued, the affected subscribers were unable to access to their own accounts.

2. The Organisation investigations indicated that the Incident was due to threat actor(s) who gained access to its IT systems through coordinated social engineering tactics targeted at staff. The threat actor(s)' aim was to use compromised staff accounts to gain control of subscriber accounts of the affected individuals to perform unauthorised activities.

3. The Organisation also made reports to IMDA under the Telecoms Act and the Singapore Police Force ("**SPF**").

4. The Organisation's investigations found no evidence that the integrity of its affected IT systems had been compromised or that any data had been exfiltrated from the systems at the time of the Incident, the Organisation had in place reasonable security arrangements that included the following:

    a. Password requirements in security policies, standards and guidelines were aligned to industry best practices;

[1] Singtel stated that the threat actor could have also accessed the records of an additional 15 subscribers.

b. Systems and network enhancements were continually implemented to improve the security of applications and IT infrastructure;

c. Comprehensive and annual mandatory training was conducted for all staff in relation to the requirements under the PDPA; and

d. Reasonable security measures were in place for the work environment of all staffs based locally and overseas.

5. The Organisation took prompt action to mitigate the effects of the breach by suspending the compromised staff accounts and by password resets. Apart from exclusion from their account for a limited duration, no other loss or damage to any individual was reported from the Incident. Remedial action to prevent recurrence will remain confidential for security reasons.

6. The Deputy Commissioner for Personal Data Protection found that the Organisation had met its Protection Obligation in the circumstances. No enforcement action therefore needs to be taken in relation to the Incident.