PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPCS 16

Case No. DP-2108-B8816

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

Personal Data Protection Act 2012

And

QCP Capital Pte Ltd

SUMMARY OF THE DECISION

1. On 30 August 2021, QCP Capital Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a personal data breach that had occurred through an unauthorised access to employee accounts and exfiltration of customer personal data (the "**Incident**").

2. As a result of the Incident, the personal data of 675 individuals was exfiltrated. The personal data affected includes name, NRIC number, date of birth, address, passport scan, passport number, photograph, email address, phone number, Telegram and WeChat ID, whitelisted address and trading records (which included the account balances, buy/sell/settlement activities).

3. The Organisation engaged an external cybersecurity company, Blackpanda Pte Ltd, to investigate the Incident. Its investigations found that the threat actor(s) had accessed two accounts, belonging to one employee, to gain unauthorised access to the Organisation systems and subsequently exfiltrated of personal data.

4. Investigations revealed that 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 also had an internal monitoring system in place which allowed the Organisation to detect, escalate the anomalous transaction, flag and suspend the trading account affected.

5. Following the Incident, the Organisation took prompt and extensive remedial action to mitigate the effects of the Incident and enhance the overall robustness of its security measures. This included notifying the affected individuals, layering access controls and introducing mandatory hardware key access authentication.

6. In view of the above, the Deputy Commissioner for Personal Data Protection is satisfied that the Organisation was in compliance with its Protection Obligation under section 24 of the PDPA and cannot be held liable for the unauthorised access by the threat actor(s) involved. 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.