PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2105-B8350

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

And

Carousell Pte. Ltd.

SUMMARY OF THE DECISION

1. On 14 May 2021, Carousell Pte. Ltd. (the "**Organisation**") informed the Personal Data Protection Commission of an unauthorized access to their users' accounts due to credential stuffing.

2. The Organisation was first alerted on 26 April 2021 when a user reported to the Organisation that his account had been hijacked and there were attempts to make unauthorised purchases. On 1 June 2021, the Organisation was alerted to another incident involving the same modus operandi where legitimate credentials were used to log in to users' accounts and unauthorised purchases were made (collectively, the "**Incident**").

3. The Organisation's investigations indicated that the Incident was due to the threat actor(s) obtaining the login details and passwords of some of their users due to an exposure of the account details on another service provider's platform. The threat actor(s) succeeded in

certain cases where the user used the same login and password for their account with the Organisation and their compromised accounts with other provider's platforms. After successfully logging into the account, the threat actor(s) was able to perform actions as an authorised user. The threat actor(s) would also have access to the data in an individual's account and modify the account settings.

4. The Organisation's investigations found that there was no known compromise or unauthorised access of information in other accounts that were stored in the same database. At the time of the Incident, the Organisation had in place security arrangements including, but not limited to, the following:

   a. Users are informed when there is a change to the password, email or phone number linked to their account, or when a new device is used to log in;

   b. Training of account takeover model to identify and investigate likely account takeovers;

   c. Card transactions that meet a certain fraud score are blocked or reviewed;

   d. One Time Password required to complete transactions for all card payments;

   e. Regular review of policies and regular testing and review of risk rules based on fraud trends, seasonality, regulation and all related indicators;

f. Company-wide training and educational newsletters to increase staff awareness on security and data protection requirements; and

g. Conduct annual penetration security assessment.

5. I am of the view that the Organisation had adopted reasonable standards for protecting personal data in their customer accounts on an objective review of the measures that were implemented at the time of the Incident. Further, the Organisation took prompt action to mitigate the effects of the breach by suspending the compromised users accounts and force password resets for affected users. Emails were sent to alert affected users of suspicious login in their accounts. DBS Paylah! Express Checkout was disabled for affected users whose accounts were suspected to have been compromised.

6. The Organisation also reviewed the Incident, and took remedial measures to enhance the robustness of their security measures, including but not limited to the following:

a. Blocked suspicious IP addresses;

b. Added rules into third party fraud detection tool to prevent account takeovers;

c. Implemented a mandatory 2FA verification, via email, in the event there is a change detected in the user's device ID across all platforms; and

d. Efforts to educate users and raise awareness to fight against phishing attempts were enhanced.

7. Having found that at the time of the Incident, the Organisation had implemented reasonable security arrangements to protect the personal data under its control, I conclude that the Organisation did not breach its Protection Obligation under the Personal Data Protection Act.