Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Carousell PTE Ltd. (Organization)
Decision number (file number)	P2023-ND-005 (File #028428)
Date notice received by OIPC	December 22, 2022
Date Organization last provided information	December 22, 2022
Date of decision	February 1, 2023
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose personal information was collected in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is based in Singapore and is an "organization" as defined in section 1(1)(i) of PIPA. The Organization is a Singaporean smartphone and web-based consumer to consumer and business to consumer marketplace for buying and selling new and second-hand goods.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • first and last name, • cell-phone number (if available), • email address, and • date of birth. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 15, 2022, the Organization completed a system migration.

	• As a result of this migration, a misconfiguration was introduced in an external-facing application programming interface (API). • As a result of the migration, a filter was inadvertently omitted and the API fetched additional details. • On September 15, 2022, the misconfiguration was discovered and fixed. • On October 13, 2022, the Singapore Data Protection Commission (PDPC) and Computer Emergency Response Team of the Cybersecurity Agency of Singapore (SingCERT) notified the Organization of an individual claiming to be selling personal data of the Organization's customers on a forum. • The Organization was able to confirm a threat actor was able to exploit that vulnerability during a 6-day period from May 7 to May 13, 2022, and again on June 25, 2022.
Affected individuals	The incident affected 2.6 million individuals, including 760 individual in Alberta.
Steps taken to reduce risk of harm to individuals	Steps taken include but not limited to: • Fixed the vulnerability upon discovery. • Reviewed all APIs, added additional restrictions and rules. • Notified data protection authorities.
Steps taken to notify individuals of the incident	The Organization notified affected individuals by email on December 15, 2022.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported, *There is a risk of phishing for all users. There is also a risk of identity theft for users whose date of birth was accessed.* I agree with the Organization's assessment. A reasonable person would consider the contact information and birthdate could be used for the purposes identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported, *There is a risk of significant harm. The organization was informed by the Singapore Data Protection Commission (PDPC) and Computer Emergency Response Team of the Cybersecurity Agency of Singapore (SingCERT) that an individual was claiming to be selling personal data of Carousell's customers on a forum.*

	I agree with the Organization's assessment. A reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The attacks appear to have been ongoing for approximately 6 days before the Organization discovered the threat.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

The contact information and birthdate could be used for the purposes identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The attacks appear to have been ongoing for approximately 6 days before the Organization discovered the threat.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email on December 15, 2022, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner