# Investigation Report

Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap 486)

## Unauthorised Scraping of the Personal Data of Carousell Users

**Report Number：R23 - 0665**

**Date of Issue: 21 December 2023**

# Investigation Report
## Unauthorised Scraping of the Personal Data of Carousell Users

Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) provides that "*the* [Privacy Commissioner for Personal Data] *may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report -*

*(a) setting out -*

*(i) the result of the investigation;*

*(ii) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and*

*(iii) such other comments arising from the investigation as he thinks fit to make; and*

*(b) in such manner as he thinks fit."*

This investigation report is hereby published in the exercise of the powers conferred under section 48(2) of the Ordinance.

**Ada CHUNG Lai-ling**
**Privacy Commissioner for Personal Data**
**21 December 2023**

# Investigation Report

Published under Section 48(2) of the Personal Data (Privacy) Ordinance
(Chapter 486, Laws of Hong Kong)

## Unauthorised Scraping of the Personal Data of Carousell Users

## I. Background

1. On 26 October 2022, Carousell Limited [1] submitted a data breach notification to the Office of the Privacy Commissioner for Personal Data (the PCPD). This notification reported that on 13 October 2022, Carousell Pte Ltd[2] (Carousell Singapore) discovered that a listing posted on an online forum offered for sale the personal data of 2.6 million Carousell users, and that on 21 October 2022, it had been found that 324,232 user accounts in Hong Kong were affected.

2. According to Carousell Limited, the data breach incident (the Incident) was caused by a security vulnerability (the Security Vulnerability) that was introduced during a system migration in January 2022 (the Migration).

3. On receipt of the aforesaid data breach notification, the PCPD immediately commenced a compliance check of Carousell Limited to ascertain the relevant facts relating to the Incident. Upon receipt of further information from Carousell Limited, the Privacy Commissioner for Personal Data (the Commissioner) concluded that Carousell Limited's acts or practices related to the Incident might have contravened the requirements of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance). In January 2023, the Commissioner commenced an

[1] A limited company registered in Hong Kong.
[2] A company based in Singapore.

investigation against Carousell Limited regarding the Incident (the Investigation), pursuant to section 38(b)[3] of the Ordinance.

[3] Section 38(b) of the Ordinance provides that where the Commissioner has reasonable grounds to believe that an act or practice has been done or engaged in, or is being done or engaged in, as the case may be, by a data user which relates to personal data and may be a contravention of a requirement under the Ordinance, the Commissioner may carry out an investigation in relation to the relevant data user to ascertain whether the act or practice is a contravention of a requirement under the Ordinance.

## II. Information Obtained from the Investigation

4. The Investigation was performed from January to October 2023. During the course of the Investigation, the Commissioner conducted five rounds of enquiries regarding the security measures adopted by Carousell Limited at the time of the Incident. Various items of information provided by Carousell Limited in relation to the Incident were reviewed and examined, including an investigation report provided by an independent information security consultant (the Consultant) engaged by the Carousell Group[4]. The Commissioner also considered the follow-up and remedial actions taken by the Carousell Group in the wake of the Incident.

5. According to Carousell Limited, the Carousell Group operates under a centralised model in which certain shared services, including security, legal and tech team services, are consolidated. Carousell Singapore controls the Carousell Group's system infrastructure and database, which is provided to entities within the Carousell Group in different regions, including Carousell Limited in Hong Kong. Carousell Limited confirms that it controls the collection, holding, processing and use of the personal data of Carousell users in Hong Kong.

Background of Carousell

6. Carousell is an online multi-category classified and recommerce marketplace for new and second-hand goods. The Carousell Group was founded in 2012 in Singapore, and Carousell is also available in Hong Kong, Malaysia, Indonesia, the Philippines and Taiwan, and has tens of millions of monthly active users.

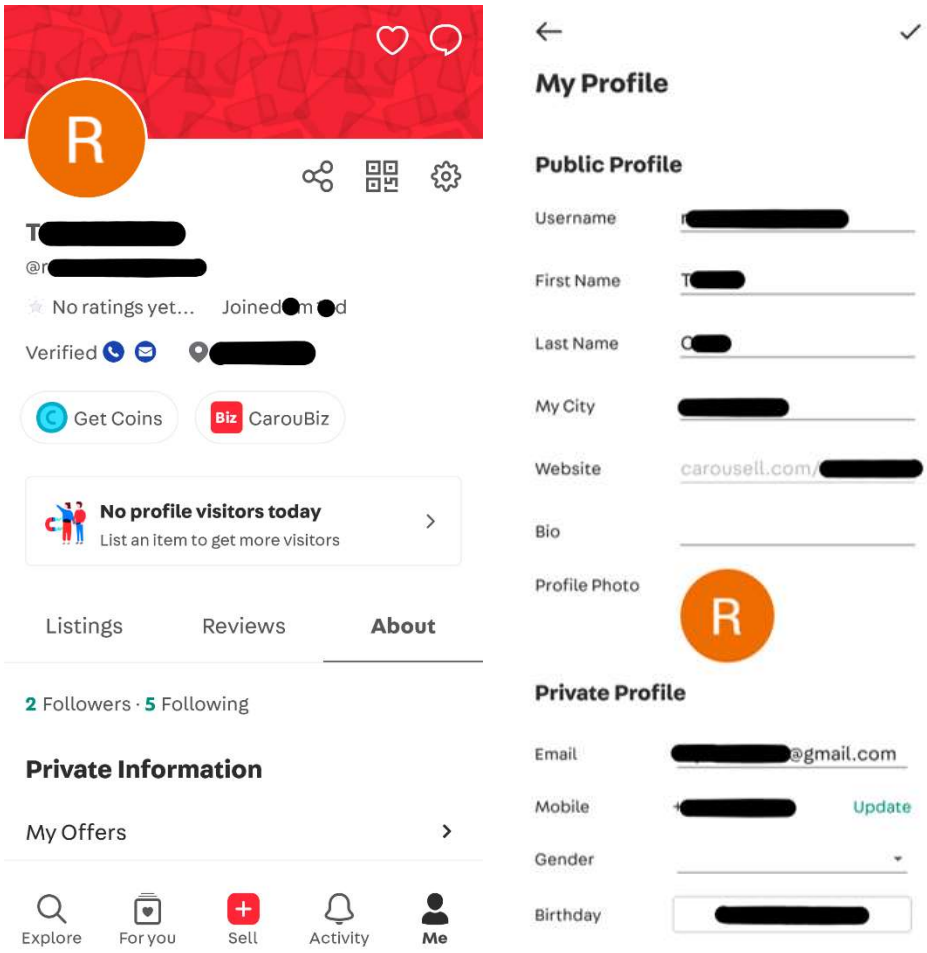
[4] The Carousell Group is the group of companies that operates Carousell, including Carousell Singapore and Carousell Limited.

7. Users who wish to buy or sell goods on Carousell may create a user account on Carousell's website [5] or its mobile application [6]. During registration, a user is required to provide his/her email address, region and mobile phone number[7]. A user may also choose to supply additional data, such as his/her first and last name, profile image, gender and date of birth.

8. The public profile of a Carousell user generally displays the user's username, first and last name, profile image and region. The private profile of a Carousell user, which is only displayed to the user, contains other personal data provided during registration. Carousell also contains social media like features that allow users to follow or be followed by other users. The number of "followers" and "following" are also shown on the user's public profile.

[5] https://www.carousell.com.hk/ (the domain for Hong Kong users)
[6] Both iOS and Android platforms.
[7] Users are required to provide their mobile phone number when using an email address to create an account on the Carousell website.

*User Profile*




Personal Data affected

9. Under section 2(1) of the Ordinance, "personal data" means any data relating directly or indirectly to a living individual, from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and in a form in which access to or processing of the data is practicable.

10. Carousell Limited submitted that the total number of user accounts affected in Hong Kong was 324,232[8]. Carousell Limited stated that apart from publicly available information contained in the public profiles of

[8] Carousell Limited claimed that individuals may have multiple accounts.

affected users (i.e. their username, first and last names and profile image), their email addresses, phone numbers and dates of birth (if provided) were also accessed and leaked in the Incident. However, Carousell Limited stated that no identification card numbers, password-related information or credit card or payment-related information were compromised in the Incident.

The Incident and the Security Vulnerability

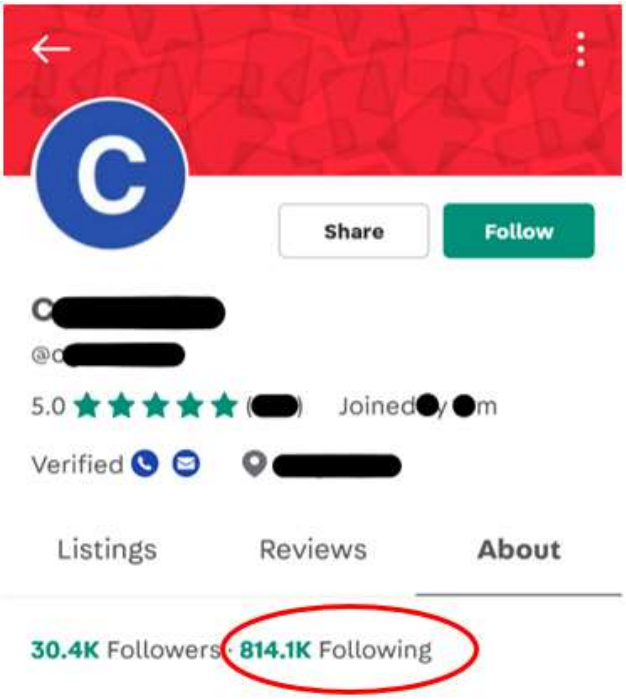
11. Carousell Limited submitted that the Carousell Group commenced the Migration in January 2022 and introduced a user-facing application programming interface (API) on 15 January 2022 as part of a gradual migration process that involved over 200 user-facing APIs. The API was intended to call up public-profile personal data on the users that a particular user is following, such as the users' usernames, names and profile image.

12. Carousell Limited explained that, due to human error, a filter (the Filter), which should have been added to remove private-profile personal data from the call up result, was inadvertently omitted during the Migration process, resulting in the API calling up additional personal data. This had not been an intended function of the API, and Carousell Limited stated that it occurred due to a coding error (the Security Vulnerability).

13. The Security Vulnerability was not noticed until a standard review process for a new feature was performed on 15 September 2022. The Carousell Group fixed the Security Vulnerability on this day to prevent unauthorised access to the data through the API and conducted an analysis for the period from January 2022 to 15 September 2022. The analysis did not find that there had been abuse of the API during this period. Accordingly, the Carousell Group considered that the Security Vulnerability was patched in time.

14. On 13 October 2022, it was brought to the Carousell Group's attention that the personal data of 2.6 million Carousell users had been placed for sale on an online platform. Based on preliminary investigations, the Carousell Group concluded that only users in Singapore were affected by this result of the Incident. However, the Carousell Group later confirmed on 21 October 2022 that users in Hong Kong were also affected.

15. According to the Carousell Group and the Consultant's forensic investigation, the attacker scraped 46 Carousell users' accounts via Internet protocol addresses of a single Internet service provider in Myanmar in May and June 2022. These 46 users were following a large number of other Carousell users, and the attacker used the 46 users' accounts to obtain the personal data of the users that they were following. The image below illustrates the profile of one of these 46 users (personal data redacted).




16. The major events that are relevant to the Incident according to Carousell Limited are set out below:

| Date/Period | Events |
|---|---|
| January 2022 | The Migration took place. |
| 15 January 2022 | The Carousell Group launched the API as part of a gradual migration process. |
| May to June 2022 | The attacker scraped 46 Carousell users' accounts and used them to obtain the personal data of the Carousell users followed by these 46 users. |
| 15 September 2022 | The Security Vulnerability was discovered and fixed. |
| 13 October 2022 | The Carousell Group discovered that the personal data of 2.6 million Carousell users were posted for sale on an online platform. |
| 14 October 2022 | The Carousell Group concluded that only users in Singapore were affected. |
| 21 October 2022 | The Carousell Group confirmed that users in Hong Kong were also affected. |

Carousell Limited's Explanation of the Incident

17. Carousell Limited admitted that the senior engineer who was responsible for and was experienced in migrating APIs had inadvertently omitted to add the Filter during the Migration, resulting in the API calling up additional personal data that it was not supposed to. Furthermore, Carousell Limited stated that their code reviewer had failed to detect this

coding error during the code review process.

18. Carousell Limited confirmed that the Carousell Group did not conduct any privacy impact assessments prior to the Migration. Carousell Limited submitted that the Migration was not a single event but a process of migrating hundreds of APIs over a period of months. The Carousell Group had previously conducted migrations of various scales during which no personal data were impacted.

19. According to Carousell Limited, upon completion of the relevant coding process of any feature and/or migration, it was the general practice of the Carousell Group to conduct a code review process followed by a testing process. However, both processes failed to detect that the Filter was missing from the API. Carousell Limited provided the following explanation:-

"*However, as this was a migration of the API, we needed to keep the contract the same so that it would be backward compatible and there would be no issues with the older clients (iOS App & Android App). Since the contract was the same, our code review process did not detect the missing filter. Our team testing process also did not detect the missing filter as the testing was based on UI and this was not a UI bug.*

*The code review process focused on the functionality of the API rather than specific security issues. At the time of the migration, we did not have security reviews for every API change, as it is not feasible for us to have a security team large enough to conduct such manual reviews.*"

20. Carousell Limited confirmed that, prior to the Incident, there had been no formal, documented guidelines relating to the code review process and the testing process.

21. In addition to the specific code review process and testing process, in February 2022 the Carousell Group engaged an external cybersecurity service provider to conduct a penetration test and security assessment to identify vulnerabilities in its web and mobile applications, as a general security measure. The Carousell Group asked the service provider why the security assessment had failed to detect the Security Vulnerability, and the service provider explained that this was because they had focused on areas that were deemed more pertinent and riskier to Carousell, and the security assessment did not cover the affected API.

22. With regard to their monitoring system, Carousell Limited stated that the Carousell Group had applied "rate limits"[9] to detect abnormal activities on its web platforms[10] and to detect the usage of APIs. During the Incident, the attacker's activities had remained below these rate limits and thus were not detected.

The Consultant's Investigation Findings

23. According to Carousell Limited, upon discovery of the Incident, the Carousell Group engaged the Consultant to investigate and identify potential malicious activity targeting the API, and determine whether the Incident could have been detected earlier.

24. The Consultant confirmed that the attacker scraped the 46 Carousell users' accounts in May and June 2022. Another attempt was made to scrape accounts in October 2022, but this was unsuccessful as the Security Vulnerability had been fixed by this time.

[9] This generally involves restricting the number of requests that can be made to a server or an API within a specified period.

[10] Website and mobile application.

25. The Consultant's investigation report included the following key findings on the Carousell Group's detection capabilities at the time of the Incident:-

(i) The code review process conducted by the Carousell Group did not include a comprehensive review of the codes for security issues, although such a review could have detected the overly permissive API implementation before its commitment to production;

(ii) The Carousell Group conducted a penetration test on the application, but this test did not identify the Security Vulnerability; and

(iii) No alert was configured to detect suspicious API usage; thus, the malicious querying was not detected by the Carousell Group.

Remedial Measures Taken by the Carousell Group

26. Carousell Limited submitted that on 13 October 2022, after becoming aware of the Incident, the Carousell Group identified the attacker, and blocked the attacker's account and all related devices and users. Subsequently, Carousell Limited submitted the data breach notification to the Commissioner and sent all affected users an email to notify them of the Incident.

27. Carousell Limited also submitted to the Commissioner that the Carousell Group had implemented a series of enhancement measures, concerning staff awareness, security measures (including detection measures) and security assessment, to prevent similar incidents from occurring in future. Details of which are not set out in this report in order to maintain the confidentiality of the security measures adopted by the Carousell Group.

## III. Findings and Contravention

Carousell Limited as the data user

28. Carousell is an online multi-category classified and recommerce marketplace that allows individuals to create user accounts via which they can buy and sell items. Carousell Limited is responsible for the operation of the Carousell marketplace in Hong Kong and uses the information systems and database under the centralised model of the Carousell Group. However, Carousell Limited confirms that it controls the collection, holding, processing and use of the personal data of the Hong Kong users impacted by the Incident. In this regard, Carousell Limited is a data user[11] as defined under section 2(1) of the Ordinance and is thus required to comply with the requirements of the Ordinance, including the six Data Protection Principles (DPPs) set out in Schedule 1 to the Ordinance.

Contravention of DPP 4(1)

29. DPP 4(1) requires that all practicable steps shall be taken to ensure that any personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to–

(a) the kind of data and the harm that could result if any of those things should occur;
(b) the physical location where the data is stored;

[11] Under section 2(1) of the Ordinance, a data user, in relation to personal data, means "*a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data*".

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
(e) any measures taken for ensuring the secure transmission of the data.

30. Having considered the facts of the Incident and evidence obtained during the course of the Investigation, the Commissioner considers that the Incident was caused by the deficiencies stated below.

*(1) Failing to Conduct a Privacy Impact Assessment Prior to the Migration*

31. The Commissioner notes that the Carousell Group has a "*Carousell Group Data Protection Impact Assessment Policy*"[12] (the Policy) which, among other requirements, outlines situations in which a privacy impact assessment should be conducted, and that the situations include "*creating a new process, including manual processes, that involves the handling of personal data*" and "*changing the way that existing systems or processes handle personal data*".

32. Since the Carousell Group introduced the API on 15 January 2022 as part of the gradual migration process which would call up personal data from the public profile of a user, their process of handling personal data has changed. However, no privacy impact assessment was conducted prior to the Migration or the introduction of the API. Carousell Limited submitted that the Migration was not a single event but a process of migrating hundreds of APIs over a period of months and that the Carousell Group had previously conducted migrations of various scales during which no personal data was impacted.

[12] Effective from April 2021.

33. The Commissioner disagrees with Carousell Limited's explanation. Considering that the Migration was a large-scale migration involving hundreds of APIs and that the introduction of the new API led to a change in the process of handling personal data of users, the Carousell Group should have paid specific attention to the security of personal data and adhered to the Policy, i.e. conducted a privacy impact assessment with the aim of thoroughly reviewing the Migration process and identifying potential privacy risks and impacts. The Commissioner considers that if the Carousell Group had adopted a prudent approach and conducted a privacy impact assessment prior to the Migration, it could have identified the potential risks and taken steps (e.g. conducted an effective security review before the launch of the API) that would have prevented the Incident from occurring.

34. The Commissioner considers that while Carousell Limited uses the centralised information systems and database provided by the Carousell Group, Carousell Limited is a data user and thus has a positive duty to safeguard the security of the personal data under its control. Therefore, it is crucial for Carousell Limited to evaluate and minimise the security risks of any migration process involving the personal data of Carousell users in Hong Kong. The absence of a privacy impact assessment and Carousell Limited's failure to check whether a privacy impact assessment had been conducted prior to the Migration exposed the personal data of Carousell users, including Hong Kong users, to a significant security risk.

*(2) Incomprehensive Code Review Process*

35. Before putting a new product or feature into production, it is essential to conduct a security assessment to identify and remove any security vulnerabilities and thereby ensure data security. The Carousell Group had conducted a code review process and a testing process after completing the

coding process of the API. However, Carousell Limited admitted that the code review process had examined the functionality of the API but had not explored for security issues and that the testing process was based on the user interface. Consequently, the absence of the Filter was not detected. Carousell Limited explained that at the time of the Migration, the Carousell Group did not conduct security reviews for every API change, as it was not feasible for it to retain a security team large enough to conduct such manual reviews.

36. As noted by the Consultant, a comprehensive review of code to detect security issues could have detected the overly permissive API implementation before committing the same to production. This is because conducting a thorough code review process to identify potential security issues is an effective way to prevent data breaches and ensure the security of an application or system. The Commissioner considers that the newly introduced API should have been subjected to a comprehensive code review process and that insufficient manpower is never a reason for not conducting such review.

37. The Carousell Group's failure to conduct a comprehensive code review process to identify potential security issues had a direct impact on all Carousell users, including its Hong Kong users. Therefore, being the data user in the Incident, Carousell Limited bore the responsibility to take all practicable measures to safeguard the personal data in its possession or control. Moreover, Carousell Limited is accountable for failing to check whether a comprehensive code review process was implemented under the data security requirement of the Ordinance, with respect to the personal data of Hong Kong users under its control.

*(3) Inadequate Security Assessment Associated with the Migration*

38. The Commissioner notes that as part of its general security measures, the Carousell Group engaged an external cybersecurity service provider in

February 2022 to conduct a penetration test and security assessment to ascertain vulnerabilities in its web and mobile applications. However, the Security Vulnerability went undetected as the penetration test and security assessment did not cover the API in question.

39. Conducting a regular and thorough security assessment on an entire system, especially subsequent to any major events (e.g. system migration), is essential for identifying security vulnerabilities and ensuring data security. Taking into account the large scale of the Migration and the function of the API in question (i.e. calling up personal data of Carousell users), the Carousell Group should have clearly instructed the service provider to conduct a security assessment of relevant APIs. If the security assessment had covered the API in question, the Security Vulnerability would have been detected and the Incident might have been avoided. The Commissioner expresses regret at the above shortcomings.

40. The Commissioner considers that the inadequacy of the security assessment associated with the Migration exposed the personal data of Carousell users, including its Hong Kong users, to significant risks. The Commissioner reiterates that Carousell Limited's failure to ensure that a thorough security assessment was conducted for the Migration constitutes a deficiency under the data security requirement of the Ordinance, insofar as the personal data of Hong Kong users under its control is concerned.

*(4) Lack of a Written Policy in Relation to the Code Review Process*

41. Human error is one of the leading causes of data breaches. Written policies setting out clear procedures can substantially reduce the risk of human errors.

42. In this Incident, the omission of the Filter was the result of a two-tiered human error: the senior engineer responsible for migrating the API inadvertently omitted to add the Filter, and the code reviewer failed to detect the coding error during the code review of the API.

43. The Commissioner notes that the Carousell Group did not have any formal, documented guidelines relating to the code review process prior to the Incident and considers that this would have led to inconsistencies in the Carousell Group's conduction of code reviews and testing. If the Carousell Group had formulated written guidelines specifying the elements/areas to be reviewed during the code review process and the standards of the review, staff members would have had a better understanding of how the code review process should be performed, which would have reduced the risk of human deviation and error.

44. In addition, as highlighted in paragraphs 35 and 36, it is essential to conduct a security assessment before putting a new product or feature into production. Thus, the Carousell Group should have stipulated in its written guidelines that a security review was part of its code review process, as this would have prevented the omission of a security assessment during the process.

45. The Commissioner notes that the Carousell Group has implemented a remedial measure after the Incident, namely an automated code review process to detect any potential leaks of personal data. This process is detailed in a newly formulated document. If this process had been in place prior to the Incident, the Security Vulnerability could have been identified at an earlier stage.

46. As noted in paragraph 34, the Commissioner considers that although Carousell Limited uses the centralised information systems and database provided by the Carousell Group, Carousell Limited is nevertheless a data

user. Thus, Carousell Limited retains a positive duty to safeguard the security of personal data under its control by implementing appropriate policies and procedures for any processes involving the handling of personal data by information systems. Therefore, the Commissioner considers that Carousell Limited shares responsibility for failing to check and ensure that there was a written policy for the code review process.

*(5) Lack of Effective Detection Measures*

47. Carousell Limited submitted that the Carousell Group had applied rate limits to detect any abnormal activities and thus prevent bad actors from accessing its web platforms and using its APIs. In the Incident, however, the attacker stayed below the rate limits, which meant that the attacker's scraping activity was not detected.

48. The Commissioner is of the view that it is crucial for organisations to deploy effective measures for detecting any signs of intrusion or attack and thereby protect its systems from data breaches. Rate limiting is not a foolproof means of preventing abuse. Specifically, as demonstrated in the Incident, determined attackers may find ways to bypass rate limits, and thus additional measures are necessary to detect potentially malicious API usage.

49. The Commissioner considers that the Carousell Group failed to implement adequate measures to detect unusual patterns or behaviours in its systems and configure alerts to detect potentially malicious API usage prior to the Incident, and that the absence of these measures contributed to the failure to prevent or detect the extraction of personal data of Carousell users from the API.

50. The Commissioner reiterates that Carousell Limited bears responsibility for the failure to ensure that effective measures were implemented to detect

abnormal activities, and that this is another deficiency in its safeguarding of data security.

Conclusion

51. Having considered all of the evidence of the Investigation, the Commissioner considers that Carousell Limited bears responsibilities for the following deficiencies:

(1) Failure to check whether a privacy impact assessment was conducted prior to the Migration. If a privacy impact assessment had been conducted prior to the Migration, it could have identified the potential risks and taken steps that would have prevented the Incident from occurring;

(2) Failure to check whether a comprehensive code review process was implemented, which led to the failure to detect the overly permissive API implementation before committing the same to production;

(3) Failure to ensure that a thorough security assessment was conducted for the Migration. If the security assessment had covered the API in question, the Security Vulnerability would have been detected and the Incident should have been avoided;

(4) Failure to check and ensure that there was a written policy for the code review process. If written guidelines had been formulated that specified the elements/areas to be reviewed during the code review process and the standards of the review, staff members would have had a better understanding of how the code review process should be performed, which would have reduced the risk of human deviation and error; and

(5) Failure to ensure that effective measures were implemented to detect abnormal activities, which contributed to the failure to prevent or detect the extraction of personal data of Carousell users from the API.

52. **Considering Carousell's extensive international operations and the vast number of active users it serves, it is reasonable to expect that the Carousell Group, including Carousell Limited, would have invested sufficient resources in ensuring the robust security of its information systems. However, the Commissioner is very disappointed to note that the occurrence of the Incident revealed fundamental failures by Carousell to ensure the security of the personal data held by the group, and that the Incident could have been avoided if some normal risk and security assessment procedures and tools had been implemented. The Commissioner regrets that these fundamental failures led to the leakage of the personal data of 2.6 million Carousell users worldwide, including over 320,000 of its users in Hong Kong.**

53. **Although Carousell Limited was at all material times using the information systems and database under the centralised model of the Carousell Group, Carousell Limited as a data user under the Ordinance has a positive duty to safeguard the security of the personal data under its control. In the present case, the Commissioner finds that there were clear deficiencies on the part of Carousell Limited to review and ensure that proper checks, policies and measures were in place in relation to the execution of the Migration, which led to the leakage of data affecting over 320,000 Carousell users in Hong Kong. For these reasons, the Commissioner considers that Carousell Limited had not taken all practicable steps in relation to the Migration to ensure that the personal data involved**

**were protected from unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) concerning the security of personal data.**

54. While the Incident reveals rooms for improvement on the part of Carousell Limited, the Commissioner is pleased to note that Carousell Limited had promptly made data breach notification to both the PCPD and the affected Carousell users, cooperated with the PCPD in its investigation, and voluntarily acknowledged its deficiencies in the Incident. After the Incident, Carousell Group is committed to learning from the Incident and has implemented various organisational and technical measures to enhance data security and prevent similar incidents from occurring in future.

## IV. Enforcement Action

55. Section 50(1) of the Ordinance provides that following the completion of an investigation, if the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, the Commissioner may serve the data user with a written notice that directs the data user to remedy and, if appropriate, prevent recurrence of the contravention.

56. Having found that Carousell Limited contravened DPP 4(1) of Schedule 1 to the Ordinance in respect of the Incident, the Commissioner exercised her power pursuant to section 50(1) of the Ordinance to serve an Enforcement Notice on Carousell Limited, directing it to take the following steps to remedy the situation and prevent recurrence of the contravention:

(1) Engage an independent data security expert to review the web and mobile applications to ensure that they are free from coding errors and known vulnerabilities;

(2) Formulate local policies and procedures to ensure the security of the personal data of Carousell users in Hong Kong, including but not limited to the policies and procedures for conducting privacy impact assessments, vulnerability scans and security assessments when significant changes are made to servers and/or applications or upon the adoption of new technologies;

(3) Formulate local policies and procedures to ensure that the security measures adopted to detect potentially malicious API usage are adequate, meet the industry standard and are regularly reviewed;

(4) Formulate local policies and procedures to ensure that policies and procedures for conducting or checking system migration and code reviews are devised and regularly reviewed;

(5) Devise effective measures to ensure staff compliance with the policies and procedures as mentioned in items (2) to (4) above;

(6) Strengthen training on data security and data protection by organising talks/seminars/workshops for all staff members at least once a year, and establish an assessment mechanism to ensure accurate understanding of the relevant course content; and

(7) Provide documentary proof to the Commissioner within two months from the date of the Enforcement Notice, showing the implementation of the above items (1) to (6).

57. Under section 50A of the Ordinance, a data user who contravenes an enforcement notice commits an offence and is liable to a maximum fine at level 5 (i.e. HK$50,000) and imprisonment for 2 years on a first conviction.

## V. Recommendation

58. Section 48(2) of the Ordinance provides that the Commissioner may, after completing an investigation and if she is of the opinion that it is in the public interest to do so, publish a report setting out the result of the investigation and any recommendations and such other comments arising from the investigation that the Commissioner sees fit to make. In this report, the Commissioner wishes to make the following recommendations on strengthening data security to organisations which may perform information system migration involving personal data.

### *(1) Carrying out Privacy Impact Assessments*

59. The Commissioner recommends that organisations conduct a privacy impact assessment before the launch of any new project, system or service that involves the handling of a considerable amount of personal data. Organisations should also conduct privacy impact assessments when significant changes are made to their systems or practices which involve the processing of personal data and upon the adoption of new technologies.

60. Conducting privacy impact assessments would help organisations to identify potential security risks at an early stage and make improvements as necessary. It would also alleviate the privacy concerns of the public and stakeholders. When carrying out privacy impact assessments, organisations should holistically review the impact on and the risks to personal data privacy and adopt adequate measures to address such impacts and risks. This would forestall or minimise adverse effects in the event of a data breach and ensure that the collection, retention, use and security of personal data are in compliance with the requirements under the Ordinance.

*(2) Develop a Migration Plan that Prioritises Data Protection*

61. Organisations should establish a clear migration plan that takes into account all data security risks associated with system migration. This should include assessing the sensitivity level of the systems and applications that need to be migrated, and determining the steps that should be taken to preserve the security of the systems and applications during and after a migration process. Clear written policies and procedures should be formulated to provide staff members with a comprehensive understanding of the implementation details to be adopted, thereby reducing the risk of human error.

*(3) Conduct Effective Vulnerability Assessments*

62. Organisations should conduct a vulnerability assessment after a system migration to identify any potential security weaknesses that could be exploited by attackers. The scope of an assessment and all necessary information associated with the systems and applications that are subject to assessment should be clearly communicated to the party conducting the assessment, whether internal or external. If external service providers are engaged, organisations should exercise due diligence to ensure that the providers are competent and give the providers clear instructions to ensure that the scope of the assessment is adequate.

*(4) Provide Relevant Employee Training*

63. Employee training is crucial for ensuring that everyone involved in a system migration process understands the importance of data security and follows best practices. If a migration involves coding, employees should be trained or guided on the best practices for conducting code reviews to preserve data security. Such training can help to ensure that staff members are equipped

with the knowledge and skills necessary to protect personal data during a migration process.

*(5) Implement an Effective Mechanism for Detecting Abnormal Activities*

64. Organisations should monitor the traffic of APIs with public interface to ensure that they detect potentially malicious activities. Apart from implementing rate limits to restrict the number of requests that can be made, organisations should also monitor known attack patterns and implement measures, such as CAPTCHA, machine learning-based anomaly detection, and threat intelligence, which can prevent similar attacks.

*(6) Formulate Localised Policies and Procedures*

65. In addition to using global policies adopted by multinational companies, organisations are recommended to formulate local policies and procedures that take into account the local environment and regulatory framework. Such policies and procedures will protect the personal data of data subjects in Hong Kong and ensure compliance with the Ordinance.

-End-