PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPC 13

Case No. DP-2209-C0166; DP-2210-C0312

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

Personal Data Protection Act 2012

And

Carousell Pte. Ltd.

… *Organisation*

DECISION

Carousell Pte. Ltd.

Lew Chuen Hong, Commissioner — Case Numbers. DP-2209-C0166 and DP-2210-C0312

28 December 2023

Introduction

1 Carousell Pte. Ltd. ("**Carousell**") runs an online marketplace website and mobile application for the buying and selling of new and second-hand goods and services (the "**Platform**"). In recent years, the Platform has expanded to include property listings. The Platform is available to users in several markets, including Singapore, Malaysia, Taiwan, the Philippines, and Indonesia.

2 In 2022, Carousell notified the Personal Data Protection Commission (the "**Commission**") of two data breach incidents:

(a) On 5 September 2022, Carousell notified the Commission of a data breach incident involving the unauthorised disclosure of the personal data of 44,477 individuals across Singapore, Malaysia, Indonesia, Taiwan and the Philippines using Carousell's Platform (the "**1st Incident**").

(b) On 17 October 2022, Carousell notified the Commission of a separate and unrelated incident involving the sale of the personal data of at least 2.6 million[1] individuals using Carousell's Platform (the "**2nd Incident**") (collectively, the "**Incidents**").

3 The Commission commenced investigations to determine Carousell's compliance with the Personal Data Protection Act 2012 ("**PDPA**") in relation to the Incidents. On 13 February 2023, Carousell requested for the investigations into the Incidents to be handled under the Commission's Expedited Decision Procedure ("**EDP**"), which the Commission acceded to. To this end, Carousell voluntarily and unequivocally admitted to the facts set out in this decision and to its contravention of Section 24 of the PDPA in respect of the Incidents.

Facts of the 1st Incident

4 Carousell's Platform includes a chat function allowing potential buyers to send and receive messages to and from listing owners on the Platform. This chat function was available for use by both individuals who had registered accounts with the Platform ("**Registered Users**") and by individuals who did not register accounts with the Platform ("**Guest Users**"). The chat function served all categories of listings on the Platform, including property listings in different countries.

[1] Carousell was unable to confirm the exact number of individuals affected. Carousell had estimated that approximately 3.389 million individuals may have been affected. However, the threat actor's listing on the online forum claimed to consist of the personal data of approximately 2.6 million individuals.

5 On 13 July 2022, Carousell implemented changes to the chat function. The change was intended to be limited to users in Philippines responding to property listings. Where such users had provided their prior consent, their first name (if the user was a Registered User), email address and phone number would be automatically appended to the message sent to the owner of the property listing.

6 However, due to human error, the changes caused the chat function to automatically append the email addresses and names of Guest Users to messages to listing owners of all categories in all markets (the "**July 2022 Bug**"). For Guest Users in the Philippines, their telephone numbers were also appended to the messages.

7 On 18 August 2022, having not identified the July 2022 Bug, Carousell implemented a fix to resolve an unrelated issue with the pre-fill functionality of the chat function ("**August 2022 Bug**"). However, these changes caused the chat function to automatically append the email addresses and names of Registered Users to messages to listing owners of all categories in all markets as well, expanding the effect of the July 2022 Bug. For Registered and Guests Users in the Philippines, their telephone numbers were also appended.

8 Carousell was eventually made aware of the August 2022 Bug via a user report sent on 18 August 2022. On 24 August 2022, Carousell implemented a fix which resolved both the July 2022 and August 2022 Bugs.

9 As a result of the July 2022 and August 2022 Bugs, the personal data of 44,477 individuals comprising email addresses of all affected users and mobile phone

numbers of users in the Philippines were disclosed without their consent. Although the names associated with users' accounts were also disclosed, the Commission accepts Carousell's explanation that these names were not necessarily indicative of actual names of the users, and are voluntarily disclosed by users on his/her own public profiles. As such, the Commission did not consider disclosure of these names relevant for assessing the breaches of the PDPA in the Incidents.

Remedial actions

10 Following the 1st Incident, Carousell took the following remedial actions:

Actions to mitigate the effects of the 1st Incident

(a) Deleted all affected personal data disclosed in the chat function by 3 September 2022; and

(b) Notified users who had written to Carousell about the 1st Incident by 6 September 2022.

Actions to prevent recurrence of the 1st Incident or similar incidents

(c) Conducted an exercise to identify corrective and preventive measures to guard against the possible recurrence of similar incidents;

(d) Revised its Service Level Agreement ("**SLA**") policy such that personal data issue reports are marked as "Severity-1" to be resolved within 8 hours. Additionally, alerts of SLA breaches will now trigger over the weekends to shorten the turnaround time for breach detection and response;

(e) Implemented an automated unit test which automatically runs on every build of the Platform to ensure that the Platform does not erroneously append any personal data in chat messages; and

(f) Implemented requirement for additional approval from the Quality / Test engineers in each team prior to implementation of new features involving users' personal data.

11 The Commission notes that Carousell did not notify all users affected by the 1st Incident as it assessed that the 1st Incident was unlikely to result in significant harm given that the disclosure was limited to basic contact information (telephone number, email address).

Facts of the 2nd Incident

12 On 15 January 2022, Carousell launched a public-facing Application Programming Interface ("**API**") during a system migration process. However, Carousell inadvertently omitted to apply a filter on that API, resulting in a vulnerability which was eventually exploited by a threat actor (the "**API Bug**").

13 The API's original intended function was to retrieve the personal data of users ("**Following/Follower Users**") followed by or following a particular Carousell user ("**Subject User**"). A filter applied to the API would have ensured that only publicly available personal data of the Following/Follower Users - user name, name and profile image – would be called up. However, due to an inadvertent omission of the filter, the

API was able to call up non-public personal data of Following/Follower Users. These comprised their email addresses, telephone numbers and dates of birth.

14 A threat actor ("**TA**") was able to exploit this vulnerability by scraping the accounts of 46 Subject Users with large numbers of associated Following/Follower Users, thereby obtaining the personal data of these Following/Follower Users. Forensic investigation revealed that the scraping of non-public data of various users occurred between 7 May 2022 and 13 May 2022, and then on 25 June 2022.

15 Carousell's internal engineering team discovered the API Bug on 15 September 2022 and deployed a patch on the same day. Carousell conducted internal investigations to determine whether there had been unauthorised access to its users' personal data in the 60-day period prior to 15 September 2022, but did not detect any anomalies within that period. They therefore remained unaware of the exploitation by the TA until 13 October 2022.

16 On 13 October 2022, Carousell was alerted by the Commission that an individual was offering the personal data of approximately 2.6 million Carousell users for sale on an online forum. Carousell conducted investigations and confirmed that the data had been exfiltrated as a result of the vulnerabilities caused by the API Bug. On 17 October 2022, Carousell notified the Commission of the data breach.

Remedial actions

17 Following the 2nd Incident, Carousell took the following remedial actions:

Actions to mitigate the effects of the 2nd Incident

(a) Deployed a fix on 15 September 2022, the same day on which the API Bug was discovered;

(b) Compiled a list of users who were following a large number of other users to identify any risk of data abuse;

(c) Identified and blocked the TA's account on 13 October 2022, the same day on which Carousell was informed of the exploitation;

(d) Notified all affected individuals by email.

Actions to prevent recurrence of the 2nd Incident or similar incidents

(e) Configured its GitHub repository to scan for and generate alerts for data leakage;

(f) Conducted a security audit for all existing APIs and implemented a systemic regular audit;

(g) Implemented an automated security audit process for API rollouts. Alerts are generated for all API code changes which involve personal data, which would result in those code changes being reviewed by the relevant teams;

(h) Implemented rate limiting follow and batch-follow APIs to prevent potential abuse by users who follow other users;

(i) Compiled a list of users following large numbers of users a day and identifying potential risks of data abuse, with the view to banning users who attempted abuse;

(j) Actively monitored API requests for abnormal behaviour;

(k) Imposed stricter IP address rate limits;

(l) Explored third-party anomalous API access solutions; and

(m) Implemented annual penetration tests for customer-facing applications.

Findings and Basis for Determination

18 Based on the circumstances of the Incidents, the Commission's investigation focused on whether Carousell had breached its obligation under section 24 of the PDPA to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**"). Carousell was determined to have breached the Protection Obligation in two respects.

Failure to conduct reasonably scoped pre-launch testing

19 Proper pre-launch testing is necessary to identify data protection risks and defects before new and updated IT features are deployed in live environments. This

has been expressly stated in the Commission's prior decisions[2] and in guidance published by the Commission.

20 The importance of properly scoped code review was highlighted in the Commission's previous decision of *Management Corporation Strata Title Plan No. 3400* [2020] SGPDPC 10 at [9]:

> "…[O]rganisations should conduct code reviews and pre-launch testing before new IT features or changes to IT systems are deployed. These processes allow organisations to pick up and rectify errors and/or flaws in the new IT features and/or systems prior to deployment. There have been a number of cases where errors in the application code resulted in the unintended disclosure of personal data or unintended access to personal data …"

21 As stated at page 5 of the PDPC's Handbook on How to Guard Against Common Types of Data Breaches ("**PDPC's Handbook**"), organisations should ensure that applications are subjected to comprehensive testing such as unit testing, regression testing, security testing, and User Acceptance Testing ("**UAT**") before deployment. A comprehensive UAT should ensure good test coverage of scenarios including possible user journeys and exception handling, which should match real-world usage. PDPC's Checklist to Guard Against Common Data Breaches ("**PDPC's Checklist**") also recommends a test suite encompassing functional and non-functional requirements and security testing.

[2] *SAP Asia Pte Ltd* [2021] SGPDPC 6, *Grabcar Pte Ltd* [2020] SGPDPC 14

22 Adequate pre-launch testing includes implementing reasonable code review. As the Commission has stated at page 3 of the PDPC’s Checklist, organisations should ““[c]onduct code review and rigorous unit testing which includes complete testing of functional requirements to verify the compliance to the requirements specs at early stage in system development lifecycle.”

23 In respect of the 1st Incident, Carousell failed to conduct reasonable pre-launch testing upon implementing its changes to the Platform’s chat function on 13 July 2022 and 18 August 2022. Specifically, Carousell admitted that, since changes were only intended to impact Registered Users in a specific category of listings (i.e. property listings in the Philippines market), testing was not undertaken to check how the changes may have affected other users and listings outside the intended category. Given that the same chat function served all categories of listings, Carousell should have conducted pre-launch testing on categories other than property listings in the Philippines market. Reasonable code reviews and testing would have detected the July 2022 and August 2022 Bugs before the changes went “live”.

24 In respect of the 2nd Incident, Carousell had selectively performed code reviews and tests during its system migration, only for certain purposes and on certain APIs. Since the function of the API relevant to the 2nd Incident was to retrieve personal data, Carousell should have identified this API and tested it for data security risks. Carousell failed to do so. Carousell admitted that prior to the 2nd Incident, it did not mandate comprehensive code reviews for security issues.

Failure to adequately document software functional and technical specifications

25 Maintaining reliable documentation on the functional and technical specifications of an application helps an organisation keep track of issues over time. It can help to provide context to historical changes and reasons why changes were made in a certain way, which would be especially important where new personnel are expected to take over work on the application. In this regard, page 5 of the PDPC's Handbook recommends organisations to:

> "**Invest effort to document all software functional and technical specifications** (e.g. program specifications, system specifications and database specifications). The usefulness of this documentation will become even more apparent over time as the original developers move on from the project and new developers take over the software maintenance and upgrading. Without proper documentation, developers often have no references to fall back on, and may end up making assumptions about code logic that could produce incorrect results."

26 In respect of the 1st Incident, lack of proper documentation contributed to the error which resulted in the data breaches. Carousell's Platform's chat function, which was essentially a chat widget and data form, served multiple purposes which were not limited to facilitating property listings in the Philippines market. Depending on the user's purposes, different form fields would be visible to the user within the chat function. The engineer who implemented the changes to the chat function on its Platform was not the original author of the function, and did not have the context

necessary to know that such changes would affect messages regarding other users and listing categories.

27 Carousell admitted that, while its handover process (at the time of the Incidents) included a document of the key features supported by the outgoing engineer, such process was otherwise undocumented and/or not directly communicated to the incoming engineer by the outgoing engineer. With regard to the 1st Incident specifically, Carousell admitted that while the handover documentation pertained to the chat function's technical aspects, it did not address how Carousell uses the function for different purposes or how changes would affect specific groups of users.

28 In respect of the 2nd Incident, the APIs involved in the system migration were built in 2016 and did not have proper documentation. Carousell admitted that, as a result, the personnel involved in the system migration may not have been aware of the need to apply the filter to the relevant API post-migration.

29 In the circumstances, it is determined that the Organisation negligently breached the Protection Obligation in the Incidents by failing to conduct adequately scoped pre-launch testing, and by failing to adequately document functional and technical specifications of its software.

The Commissioner’s Decision

30 In determining whether to impose a financial penalty on Carousell pursuant to s 48J of the PDPA, and the amount of any such financial penalty, the factors listed at s48J(6) of the PDPA were taken into account.

31 The Commission recognises that:

(a) Carousell was cooperative with the Commission’s investigations;

(b) Carousell took prompt and effective remediation actions upon discovery of the July 2022 and August 2022 Bugs in the 1st Incident, and the API Bug and the data exfiltration in the 2nd Incident; and

(c) Carousell has not previously contravened the PDPA.

32 The Commission also recognises that the TA in the 2nd Incident was particularly sophisticated in avoiding the security measures Carousell had implemented. Carousell had, prior to the 2nd Incident, put in place API processes and security measures, such as rate-limiting and traffic monitoring against API vulnerabilities. Carousell’s security measures in respect of detecting anomalies and/or abuse of its APIs were found to be adequate in general. Despite these measures, the TA took actions to remain undetected.

33 The Commission’s investigations were handled under the EDP, under which Carousell admitted to the facts set out in this decision and to its contraventions of the

Protection Obligation in the context of the Incidents. The Organisation's early admission of liability for its breaches of the Protection Obligation is considered a significant mitigating factor. An organisation that voluntarily admits to its non-compliance with the PDPA and takes measures to correct such non-compliance is an organisation that demonstrates that it can be responsible for the personal data in its possession or under its control[3].

34 Based on the above assessment, the Commission determines that a financial penalty of $58,000 should be imposed on Carousell.

Directions

35 While Carousell implemented technical measures to correct specific issues that resulted in the Incidents, it should also review its internal processes for software testing and documentation to address the failures identified above.

36 Accordingly, the Commission hereby directs Carousell to carry out the following within 90 days:

(a) Review its software testing procedures;

(b) Review its processes and procedures for documenting functional and technical specifications of software;

(c) Rectify any gaps identified from the reviews above; and

[3] See Section 11(2) of the PDPA.

(d) Furnish to the Commission a report of the reviews and rectification actions taken in response.

DENISE WONG
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION