PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2106-B8446

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

Personal Data Protection Act 2012

And

Crawfort Pte. Ltd.

SUMMARY OF THE DECISION

1. On 9 June 2021, Crawfort Pte. Ltd. (the "**Organisation**") notified the Personal Data Protection Commission (the **"Commission"**) of the sale of the Organisation's customer data on the dark web (the **"Incident"**).

2. The personal data of 5,421 customers were affected. The datasets affected comprised NRIC images (front and back), PDF copies of loan contract (containing all the information in the NRIC, age, email address, contact number and loan amount) and PDF copies of income document (payslip, CPF statements or IRAS Notice of Assessment).

3. The Organisation engaged external cyber security teams to investigate the Incident. The investigation identified an opened S3 server port in the Organisation's AWS environment as the cause of the Incident.

4. The Organisation explained that it had opened the S3 server port for **one week** during a data migration exercise sometime on or about 15 April 2020 for business continuity purposes. On 3 April 2020, the Singapore government had announced that the country will enter into a Circuit Breaker to contain the spread of COVID-19. All non-essential workplaces, including the Organisation, had to be closed from 7 April 2020. In order to continue its business, the Organisation had to pivot its operations so as to allow its staff to work from home and its customers to make loan applications remotely. Within a very short period, the Organisation had to carry out the data migration exercise and as a result, overlooked conducting a risk assessment prior to conducting the data migration exercise.

5. The opened S3 server port connected directly to the S3 server hosting the S3 buckets, which contained the affected personal data. The open remote port enabled attempts to connect to the Organisation's AWS environment from the internet. Furthermore, the S3 bucket containing the affected personal data was publicly accessible due to a misconfiguration of the S3 bucket. As a result, the threat actor was able to gain access to the publicly accessible S3 bucket **during the one-week period**.

6. The Organisation the following remedial measures after the Incident:
    a. Reset and reconfigured all whitelisted IPs to AWS server;
    b. Reset and reconfigured all VPNs;
    c. Limited the whitelisted IP addresses to its web portal;
    d. Conducted a penetration test;
    e. Monitored the dark web to ensure that data was not circulated;
    f. Engaged independent cyber security consultant to carry out investigation, study the IT infrastructure and propose improvements to their systems; and
    g. Notified affected individuals.

7. The Commission accepted the Organisation's request for this matter to be handled under the Commission's expedited breach decision procedure. This meant that the Organisation had voluntarily provided and unequivocally admitted to the facts set out in this decision. The Organisation also admitted that it was in breach of section 24 of the Personal Data Protection Act (the "**PDPA**").

8. The Organisation admitted that it failed to conduct a reasonable risk assessment before carrying out the data migration exercise. There was no access control to the S3 bucket containing the affected personal data during the week-long migration exercise. This, coupled with the open port, allowed the threat actor to gain access to the affected personal data.

9. In the circumstances, the Organisation is found to be in breach of section 24 of the PDPA.

10. Having considered the circumstances set out above and the factors listed in section 48J(6) of the PDPA, including (i) the Organisation's upfront voluntary admission of liability which significantly reduced the time and resources required for investigations; and (ii) the prompt remedial actions undertaken by the Organisation, the Commission considered that it would be most appropriate in lieu of imposing a financial penalty, to direct the Organisation to comply with the following:

    a. To engage qualified security service provider to conduct a thorough security audit of its technical and administrative arrangements for the security and maintenance of its AWS S3 environment that contains personal data in the Organisation's possession or control;
    b. Provide the full security audit report to the Commission, no later than 60 days from the date of the issue of this direction;
    c. Rectify any security gaps identified in the security audit report, review and update its personal data protection policies as applicable within 60 days from the date the security audit report is provided; and
    d. Inform the Commission within 1 week of completion of rectification and implementation in response to the security audit report.

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.