PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2011-B7387

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

And

Giordano Originals (s) Pte Ltd

SUMMARY OF THE DECISION

1. On 3 December 2020, the Personal Data Protection Commission (the "**Commission**") was notified by Giordano Originals (S) Pte Ltd (the "**Organisation**") of an unauthorized network entry and ransomware infection at the OS and server level that occurred on or about 12 July 2020 (the "**Incident**").

2. As a result of the Incident, two of the Organisation's systems, one which stores the personal data of its employees and second, the personal data of its members were affected.

3. The Organisation's own and independent investigation conducted found no sign of suspicious activity in the Singapore network, and no impact beyond the Singapore network. The unauthorised entry had most likely occurred through the use of compromised credentials obtained through phishing.

4. Personal data of 790,000 members and 184 employees in encrypted form were affected. The personal data of members comprised names (20% of the members), contact number and partial date of birth (without birth year). The personal data of employees comprised name, NRIC, address, gender, age, contact number, email address, educational and salary information.

5. Investigations revealed that the Organisation had in place reasonable security measures that are consistent with the recommendations that the Personal Data Protection Commission had made in our recent Handbook on “How to Guard Against Common Types of Data Breaches” on how to prevent malware or phishing attacks. The Organisation had installed and deployed various endpoint security solutions, which was complemented with real-time system monitoring for any Internet traffic abnormalities. Even before the Incident, the Organisation also conducted regular periodic system maintenance, reviews and updates (such as vulnerability scanning and patching).

6. More importantly, the Organisation had also ensured that its data was regularly and automatically backed-up, which was a key recommendation that the Commission made in our Handbook.

7. In addition, the Organisation had also taken steps to better protect the personal data affected by encrypting the personal data using current industry-standard RSA algorithm and passphrase. As a result, the personal data affected by the ransomware was not legible without decryption.

8. The Commission endorses the proper use of industry-standard encryption to protect personal data, and will give due weight to Organisations which have implemented the recommendations we made in our Handbook in determining whether an organisation has complied with its Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”), or as a strong mitigation factor in the event of the Commission finds that there has been a breach of section 24 of the PDPA.

9. Following the Incident, the Organisation took prompt and extensive remedial both to mitigate the effects of the Incident and enhance the robustness of its security measures. This included increased frequency of staff phishing simulation trainings and security reviews as well as additional monitoring measures. There was no evidence of exfiltration of the personal data or decryption of the personal data. The Organisation was also able to fully restore the personal data from its backups.

10. In light of the reasons discussed above, the Deputy Commissioner for Personal Data Protection is satisfied that the Organisation had met its Protection Obligation under section 24 of the PDPA. In light of our findings, we will not be issuing any directions or taking any further enforcement action against the Organisation in relation to the Incident.