PERSONAL DATA PROTECTION COMMISSION

Case No. DP-1905-B3820

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

And

Novelship Pte. Ltd.

SUMMARY OF THE DECISION

1. Novelship Pte. Ltd. (the "**Organisation**") operates an e-commerce website for individuals to sell or buy luxury brands of streetwear (the "**Website**"). To create a buyer or seller account on the Website, individuals would have to provide their personal data to the Organisation. The Organisation does not, in usual course, reveal the personal data it had collected to any buyer or seller transacting on the Website. Instead, the Organisation, together with an external payment processor, facilitates transaction payments on behalf of the parties.

2. On 1 May 2019, the Personal Data Protection Commission (the "**Commission**") received information that a registered seller ("**User**") was able to gain unauthorised access to the personal data of other sellers by employing software tools and manipulating the public URLs of active listings ("the "**Incident**").

3. The User had accessed the personal data of six unique sellers who had active listings at the time of the Incident. The personal data concerned included: (i) first and last names; (ii) email addresses; (iii) shipping addresses; (iv) hashed account passwords; and (v) the name of bank and bank account numbers ("**Personal Data Sets**"). No buyer data was accessed in the Incident.

4. Investigations revealed that the Organisation had not conducted adequate security testing before the launch of the Website. The testing it had conducted was limited to design and functionality issues, such as verifying the password hashing and password requirement functions. **Critically, the Organisation should have—but had not—conducted vulnerability scanning**. Vulnerability scanning that is reasonably and competently conducted should include scanning for OWASP Top Ten, i.e. the top 10 security vulnerabilities listed by the Open Web Application Security Project ("**OWASP**"). The vulnerability of URLs to manipulation is within the OWASP Top 10, and would have been detected if the Organisation had conducted adequate vulnerability testing.

5. The Commission understands that not every organisation is equipped with adequate knowledge of cyber security risks or the ability to conduct security testing. However, the obligation of organisations to protect the personal data they collect and process online cannot depend on their subjective familiarity with the security risks or ability to prevent them. Organisations are expected to engage qualified competent parties, where reasonably needed, to assist them to discharge their obligation to protect personal data. When doing so, organisations can refer on the technical advice and expertise of their service provider, but remain ultimately responsible for articulating the business risks they wish to avoid and business outcomes that they seek to achieve.

6. Similarly, the Commission recognises that organisations may face financial, manpower and technical limitations. These limitations are relevant in establishing the reasonableness of decisions they have taken, but cannot allow an organisation to justify providing a level of protection that is below what is reasonable for the type of personal data it collects and processes.

7. Accordingly, the Deputy Commissioner for Personal Data Protection finds the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012.

8. Having considered the representations made by the Organisation and the material factors, in particular:

   (a) the sellers' personal data would have been at risk of unauthorised access for a period of eight months (from the time the sellers were first allowed to sell on the Website, to the date remedial actions were taken);

   (b) there was actual unauthorised access of the Personal Data Sets of six individuals by the User;

   (c) the remedial measures taken by the Organisation upon being made aware of the Incident; which included fixing the vulnerability to ensure that the sellers' personal data would no longer be accessible to unauthorised persons, redacting all user information relating to bank information, and the Organisation committing to developing a new website; and

   (d) the adverse impact the COVID-19 pandemic had on the Organisation's business;

   the Deputy Commissioner for Personal Data Protection directs that the Organisation pays a financial penalty of S$4,000 for the contravention. The Organisation must make payment of the financial penalty within 30 days from the date of this direction, failing which interest, at the rate specified in the Rules of

Court in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until it is paid in full. No other directions are required as the Organisation had implemented the necessary remedial measures.