WRITTEN VOLUNTARY UNDERTAKING ("Undertaking")
TO THE PERSONAL DATA PROTECTION COMMISSION

This Undertaking is given to the Personal Data Protection Commission or its delegates pursuant to section 48L(1) of the PDPA, by:

Simmons (Southeast Asia) Private Limited
UEN: 199303272D
Registered Address: 300 Beach Road, #25-03, The Concourse, Singapore 199555

(hereinafter referred to as the "**Organisation**").

By signing this Undertaking, the above-named Organisation acknowledges the matters stated herein and undertakes to the Commission in the terms set out herein.

1. DEFINITIONS

In this Undertaking:

(a) "**PDPA**" means the Personal Data Protection Act 2012; and

(b) "**Relevant Provisions**" means the provisions in Parts III, IV, V, VI, VIA and IX, and section 48B(1) of the PDPA.

2. ACKNOWLEDGEMENTS

2.1 The Organisation hereby acknowledges the following matters:

(a) The Commission has carried out investigations into certain acts and practices of the Organisation, and has reason to believe that the Organisation has not complied, is not complying, or is likely not to comply with one or more of the Relevant Provisions. The relevant facts and circumstances are summarised at Schedule A.

(b) As a result of any non-compliance with the PDPA by an organisation, the Commission has a number of enforcement options under the PDPA, including the option to issue directions under sections 48I or 48J of the PDPA.

(c) The Commission recognises that the Organisation has made efforts to address the concerns raised in this case and to improve its personal data protection practices. In addition, the Organisation was cooperative in the course of the investigation and was responsive to requests for information. The Commission further recognises that the Organisation

appears ready to implement or is in the midst of implementing the steps set out in Schedule B.

(d) Having carefully considered all the relevant facts and circumstances, the Commission takes the view that this is an appropriate case in which an Undertaking may be accepted.

2.2 The Organisation also acknowledges and agrees that the Commission may publish and make publicly available this Undertaking, and without limitation to the foregoing, the Commission may issue public statements referring to this Undertaking and/or its contents in whole or in part.

3. UNDERTAKINGS

The Organisation undertakes that it has taken, or will take all necessary steps, to carry out the actions or refrain from carrying out the actions referred to in Schedule B, and where applicable, in accordance with the stipulated timelines.

4. COMMENCEMENT

This Undertaking shall take effect upon the acceptance by the Commission of the Organisation's duly executed Undertaking.

5. THE COMMISSION'S STATUTORY POWERS

5.1 In order to provide the Organisation with an opportunity to complete all necessary steps to implement its undertakings set out in clause 3 above, the Commission will exercise its powers under section 50(3)(ca) of the PDPA to suspend the investigations referred to in clause 2 on the date the Undertaking takes effect as set out in clause 4.1.

5.2 The Organisation acknowledges that the Commission will verify the Organisation's compliance with its undertakings set out in clause 3 above, and if necessary, will exercise its powers under the Ninth Schedule of the PDPA to do so.

5.3 Clause 5.1 above shall be without prejudice to the Commission's statutory powers to conduct or resume, at any time, the investigations referred to in clause 2 above if it thinks fit, including but not limited to the situation where the Organisation fails to comply with this Undertaking or part thereof in relation to any matter.

5.4 Nothing in this Undertaking, including the Commission's acceptance of the Undertaking, is intended to, or shall, fetter or constrain the Commission's rights and statutory powers (including but not limited to those under sections 48I, 48J, 48L(4) and 50 of the PDPA) in any manner. Neither shall be construed as

creating any anticipation or expectation that the Commission will take or not take any particular course of action in the future (whether in the present case or in respect of any other case concerning a breach or suspected breach of the PDPA). The acceptance of this Undertaking is strictly confined to the particular facts of the present case, and is made on the basis of the representations and information provided by the Organisation. The acceptance of an Undertaking in this case shall not be construed as establishing any precedent.

6. VARIATION

This Undertaking may be varied only with the express written agreement of the Commission.

This document has been electronically signed. The Parties hereby affirm that the electronic signatures have been affixed with the due authorisation of each Party and that Parties intend for the electronic signatures to carry the same weight, effect and meaning as hand-signed wet-ink signatures.

SIGNED, for and on behalf of)

Simmons (Southeast Asia) Private Limited)

By the following:)

Name: _____)

Designation: _____)

Date: _____)

ACCEPTED by)

)

Name: _____)

Designation: _____)

Personal Data Protection)

Date: _____)

SCHEDULE A

SUMMARY OF FACTS

1. On 17 August 2022, the PDPC was informed that a server which the Organisation's and set up for testing purposes was subject to a ransomware attack, resulting in the encryption of a backup copy of its database.

2. As a result, the personal data of 87,824 customers including their name, address, email address, telephone number, and transaction information was encrypted. In addition, the data of another 128 employees, including their name, business email address, and user ID and password for internal software accounts was also encrypted. There was no evidence of any exfiltration of personal data.

3. To prevent a recurrence of a similar incident, the Organisation took immediate remedial action to address the possible cause of the personal data breach.

SCHEDULE B

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
Technical Remediation			
1.	The attacker(s) likely accessed the test server through the RDP port which was opened to public internet access.	SPL reformatted and restored the affected test server to a pre-infected version.	11 August 2022 (completed)
2.		SPL closed the RDP port of the test server from public internet access.	10 August 2022 (completed)
3.		SPL will ensure that any connection to any of SPL's servers within its IT environment can only be made through a SSL/VPN or IPSec connection, and that all RDP ports on all its servers are closed to public internet access.	12 August 2022 (completed)

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
4.		SPL has issued a SSL/VPN account to its vendor for the vendor to connect to SPL's network before accessing the test server.	12 August 2022 (completed)
5.		SPL has shut down the test server and will not reactivate the test server for development work until the appropriate security measures are implemented.	22 August 2022 (completed)
6.	SPL used production data on a test server.	SPL will remove all production data containing personal data from test servers and ensure that any future test servers will	13 September 2022 (completed)

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
		not contain personal data in any form, and will only utilise test data from which personal data cannot be derived.	
7.		SPL will set up all future test servers on a separate domain so that the possibility of lateral movement is minimised. SPL will include this as a requirement in the written internal policies/processes to be published under SN14 below.	When required.
8.	Since the test server was a new server set up solely for development work, SPL's existing	SPL will ensure that the passwords used on test servers (including the current test server) comply	25 October 2022

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
	password policy was not implemented.	with SPL's existing password policy. SPL will also require all employees to use password generation and management software to ensure that passwords are "random" and do not contain easily guessable words (e.g. SPL's name). SPL will include this as a requirement in the written internal policies/processes to be published under SN14 below.	

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
9.		SPL will also implement multi-factor authentication for all possible account logins (including administrators) in SPL, including accounts on test servers.	29 November 2022
10.	As the test server was a new server, it was not connected to SPL's Symantec Endpoint Protection system. SPL only has Symantec Endpoint Protection system in place and does not have in place any other intrusion	SPL will research on available IDS/IPS in order to implement and integrate a suitable IDS/IPS into is systems. SPL will review its current logging locations and strategies as well as look into available logs. SPL will evaluate logging solutions in order to pick a	29 November 2022

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
	detection or prevention detection systems.	solution that would best fit the organization.	
11.		SPL will ensure that SPL's endpoint protection / intrusion detection / prevention detection systems is installed on all servers and endpoints, regardless of whether they are production or test servers/endpoints, at the time the server or relevant machine is set up. SPL will include this as a requirement in the written internal policies/processes to be published under SN14 below.	When required

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
12.	The personal data that was uploaded onto the test server was not encrypted.	All personal data stored in any of SPL's servers will be encrypted.	Ongoing. Encryption of data stored on SPL's human resources server has been completed. Encryption of other servers will be completed by 15 November 2022
13.		SPL informed all users to change the passwords for all their accounts in SPL's IT environment. SPL thereafter enforced this by manually expiring	18 August 2022 (Completed)

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
		all the passwords within SPL's control, such as for the user domain accounts, SAP accounts, and SSL/VPN accounts. Out of an abundance of caution, SPL also informed all users to change the passwords of any accounts which used a SPL domain address.	
<u>Policies/Process Remediation</u>			
14.	There were no written polices / processes/ guidelines relating to the collection, use, disclosure, protection, and retention of	SPL will review and update its internal policies/processes relating to the collection, use, disclosure, protection, and retention of personal data	17 October 2022

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
	personal data in the possession and/or custody of SPL and/or its employees in place.	in the possession and/or custody of SPL and/or its employees, including but not limited to ensuring the proper documentation of the policies and processes and enhancing training for all staff on their data protection obligations	
15.	Strengthen incident response plan	SPL will draft an Incident Response Plan. The Incident Response Plan will outline the plan for responding to information security incidents containing the following information: a. Scope;	10 October 2022 (Completed)

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
		b. Incident Response Methodology; c. Incident Response Phases; d. Guidelines for the Incident Response Process; and e. Documentation, Tracking and Reporting.	
16.	There was no written contract in place with SPL's IT Vendor regarding the IT Vendor's provision of hosting services to SPL, which could include provisions for the protection of personal data.	SPL will endeavour to enter into a written contract with its IT Vendor which contractually obliges the IT Vendor to protect the personal data stored by SPL. Alternatively, SPL will endeavour to enter into a written agreement with a	SPL will either enter into a written agreement with its IT Vendor or determine if it will switch to a new vendor by 1 November 2022. If SPL determines that it should enter

No.	Potential Risk Factors/Improvement Areas	Remediation Plan	Target Completion (Date)
		different vendor on terms which oblige the vendor to protect the personal data stored by SPL.	into a written agreement with a different vendor, SPL will do so by 15 November 2022.
17.	Vulnerability testing	SPL will research on available vulnerability testing solutions in order to conduct a suitable penetration test after the above mentioned steps are taken. SPL will also implement periodic penetration testing.	29 November 2022