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:

Asia Petworld Pte. Ltd.
UEN: 201409741H
Registered Address: 2 Woodlands Sector 1, #03-18, Woodlands Spectrum, Singapore 738068

(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

1.1 In this Undertaking:

(a) "**PDPA**" means the Personal Data Protection Act 2012 (No. 26 of 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

3.1 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

4.1 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

6.1 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)

Asia Petworld Pte. Ltd.)

By the following:)

Name: _____)

Designation: _____)

Date: _____)

ACCEPTED by)

)

Name: _____)

Designation: Deputy Commissioner

Personal Data Protection)

Date: _____)

SCHEDULE A

SUMMARY OF FACTS

1. On 8 September 2021, the PDPC received a data breach notification from the Organisation concerning an unauthorised access to its systems (the "**Incident**"). The threat actor had, amongst others, deleted the Organisation's servers, including its backup servers and backup data. Consequently, the personal data of up to 21,060 individuals, including the Organisation's retail customers, former and current employees, were at risk of being accessed and subject to exfiltration.

2. The affected personal data comprised the name, address, telephone number and email address for the retail customers. As for the employees, the affected personal data consisted of name, date of birth, NRIC number or FIN, bank account number and amount(s) paid to them.

3. The Organisation did not receive any feedback from both the retail customers and the employees on this Incident on any actual financial loss and/or mis-use of the affected personal data. It had also taken steps to contain the Incident and put in place measures to prevent recurrence.

SCHEDULE B

REMEDIATION PLAN

S/N	Potential Risk Factors/Improvement Areas	Remedial Actions/Measures	Completion Date
1	Suspected malware / infected PCs / desktops in the warehouse and office	Reformat of every PC / desktop in the warehouse and office, and installed a clean Windows 10 environment, to ensure removal of all infected environment or PCs	end Aug 2021
2	PCs / Desktops were infected with malwares, and unauthorised access from the networks	Deployed BitDefender *[redacted for confidentiality]* Security Suite on every PC / Desktop and servers, to further protect the PCs / Desktops / Servers	2nd week Aug 2021
3	Easily hacked passwords on PCs / Windows Login	Compulsory reset of all users' / windows' passwords, and the need for all user password to be at least 20 characters long, with compulsory complexity requirements for passwords to include symbols, numbers, caps, and non-sequential or non-word-like passwords. Mandatory change passwords every 60 days. Do not store password in plain text anywhere in the computer / network. Apply security password on documents with personal data such as payroll worksheet when transmitted over the internet.	1st week Aug 2021
4	User / Windows accounts might have been	Enable 2FA on all available applications and services, to	2nd week Aug

	accessed without the users' knowledge	ensure that only authorised users are accessing the services assigned to them	2021
5	As we have employees across the region, and the need for smooth access of the ERP application for these users	Implement *[redacted for confidentiality]* web remote access users with 2FA - this is to ensure that only the authorised users are able to access their application securely without worry of their applications being accessed by unauthorised users	2nd week Sep 2021
6	The need to have more secure server environment	Moving of key applications to *[redacted for confidentiality]* Web Service for improved security. Implementing a new web based system which also supports 2FA and users won't have to connect to our network. So the network will be completely isolated for staff as they can work directly from the browser to access the ERP system.	1st week Feb 2022. New ERP is in the testing phase
7	Suspected less secure firewall at APPL network	Hardening the Firewall security settings at the router level by Allowing only ip's from our staff to access the network and only ports opened are those which are required for the systems to work and connect	1st week Aug 2021
8	Suspected unauthorised access remotely by intruders after office hours	Requested all users to shut down all PCs / desktops / workstations at the end of business day	end Aug 2021
9	Suspected intruders were aware of all the user accounts in APPL	Delete all domain users account and recreate new user IDs, as we need to ensure that the intruders are unable to access these user accounts remotely	2nd week Sep 2021
10	Suspected malwares were injected into the network through	Locked down all USB ports to prevent use of USB ports	1st week Aug 2021

	unauthorised plug-ins of mobile phones or USB drives into PCs/desktops		
11	Gaps in knowledge on computing and safe use of emails, and proper use of authentication software	Additional staff training for use of internet things. Moved email system to cloud based system *[redacted for confidentiality]* with 2FA enabled on it.	Sept 30, 2021
12	HR awareness training in personal data, safety and cyber security knowledge	Scheduled monthly training and updates on 3rd week of each month	October 31, 2021
13	Strengthen incident response plan, to have tabletop exercise regularly, SOPs on data management and IT management	Appointed *[redacted for confidentiality]* to be the person in charge to ensure all personnel adhere to APPL SOPs for data and IT management: 1) Login to Windows as domain user 2) Check for Windows Update 3) Login to ERP Software 4) Login to Email on Cloud 5) Check to ensure BitDefender is up-to-date 6) At the end of business day, logoff from ERP, Cloud Email, and shut down Windows	October 31, 2021
14	Hardening of system access	Enhance systems access controls and hardening of systems (Regular patching, Logs management, Backup process and restoration, etc.) and segregation of duties, tightening privileged accesses and controls	October 31, 2021