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:

JT Legal LLC
UEN: 201706016E
Registered Address: 12 Marina Boulevard #17-01 Marina Bay Financial Centre, Tower 3, Singapore (018982)

(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)

JT Legal LLC)

By the following:)

Name: _____)

Designation: _____)

Date: _____)

ACCEPTED by)

)

Name: _____Yeong Zee Kin_____)

Designation: Deputy Commissioner / Commissioner
Personal Data Protection)

Date: _____)

SCHEDULE A

SUMMARY OF FACTS

1. On 4 June 2021, the Organisation was subjected to a phishing attack where a phishing email was sent twice to joshua@jtlegal.com from no-reply@dropbox.com with the following subject: “Jaya Shakila wants to access your file “JT Legal LLC New Details.pdf”.

2. As a result of the attack, the personal data of the Organisation’s approximately 1,006 users including their name, residential address, email address, NRIC numbers and passport numbers were affected.

SCHEDULE B

S/N	Item	Status	Target Date of Completion (Month-Year)
1.	**Implementation of Multi-Factor Authentication** Multi-Factor Authentication ("MFA") will be implemented for all user accounts of the organisation.	Completed	Jul-21
2.	**Implementation of a dedicated anti-virus on computers within the organisation** Anti-virus software is to be installed on all organisation computers to increase the organisation's protection and security to external cyber threats.	In progress	Aug-21
3.	**Cyber security awareness & competency** The organisation will conduct periodic unannounced tests to assess the competency of staff in recognising and responding to potential phishing attempts.	In progress	Aug-21
4.	**Training of staff to develop cyber security awareness and competency** The organisation will develop basic cyber security training for staff of the organisation to be conducted on an annual basis to ensure that staff possess a reasonable level of cyber security competency. New staff to the organisation are to complete the mandatory basic cyber security training.	In progress	Sep-21
5.	**Protection of key data sheets** Key data sheets containing collations of personal data collected by the organisation in the course of its business will be encrypted with a password.	Completed	Jul-21

	Access to such key data sheets will be provided on a need to know basis.		
6.	Immediate remedial actions taken: a. Change of all passwords for all user accounts; b. Change of all passwords for all online databases, cloud-based services, subscription-based services and programs used by the organisation as an added security measure; c. Virus scans conducted on the computers used to access the breached email account of the organisation; and d. Anonymisation of personal data stored on the organisations' key data sheets containing collations of personal data where possible.	Completed	Jun-21
7.	**Review of internal data collection procedures and policy** A review of the organisation's internal data collection policies will be conducted to ensure that personal data will not be unnecessarily collected or retained. A review of the organisation's internal data collection procedure will be conducted to ensure personal data collected in the course of its business are properly stored and anonymised if unnecessary. Development of the organisation's password policy to ensure strong passwords are employed by the organisation.	In progress	Sep-21

8.	**Reformat of possible breached computers** The organisation will reformat computers of the organisation that had been used to access the email that had been breached.	In progress	Aug-21
9.	**Professional review of IT infrastructure and systems and subsequent implementation of further actions recommended** Engagement of an IT service professional to review the organisation's current IT infrastructure and systems to further prepare and prevent against future cyber-attacks. Implementation of further security measures as recommended by the engaged IT service professional to upgrade the organisation's cyber security measures.	In progress	Nov-21
10.	**Development of an internal reporting system** Potential phishing attempts or emails containing malware sent to an individual in the organisation are reported so that all staff are kept updated and may be kept abreast of the potential security risk. All staff have been heavily encouraged to seek assistance if they are unsure whether an email may be a phishing attempt or if they are unable to ascertain whether an email may contain malware or a link to a suspicious internet domain.	Completed	Jul-21