VOLUNTARY UNDERTAKING UNDER
SECTION 48L OF THE PERSONAL DATA PROTECTION ACT 2012

Case number: DP-2209-C0193

In the matter of an investigation under section 50(1)

of the Personal Data Protection Act 2012 ("the Act")

And

(1) Starbucks Coffee Singapore Pte. Ltd. (UEN No. 198800670D)

… Organisation

The Commission has reasonable grounds to believe that the Organisation has not complied, is not complying or is likely not to comply with section 24 of the Act. In order for the Commission to suspend its investigation pursuant to section 50(3)(ca) of the Act, the Organisation HEREBY UNDERTAKES that it will:

(a) Complete the remediation plan set out at Schedule B within the timelines stated in Schedule B; and

(b) Within 14 days of the completion of the remediation plan set out at Schedule B, provide the Commission with a copy of the declaration set out at Schedule C duly signed by the signatory of this Undertaking or a representative of the Organisation of equal designation.

The Organisation acknowledges that the Commission shall be entitled to publish and make available to the public this Undertaking and the summary of the Commission's findings set out at Schedule A to this Undertaking.

The terms of this Undertaking may be varied by the written agreement of the Commission and the Organisation.

SIGNED, for and on behalf of)

Starbucks Coffee Singapore Pte. Ltd.)

By the following:)

Name: _____)

Designation: _____)

Date: _____)

SCHEDULE A

SUMMARY OF FACTS

1. On 15 September 2022, the Commission was informed that personal data purported to be from the Organisation's Singapore customers were available on the dark web.

2. Investigation revealed that the above-mentioned personal data were indeed from the Organisation's customer database and this database were handled by Ascentis Pte. Ltd ("Ascentis"), an external vendor contracted to provide IT solutions since year 2014.

3. The cause of the data breach incident was due to lapses within Ascentis and its overseas vendor which led to a compromise of an administrator account with access to the Organisation's customer database. As a result, the personal data of approximately 332,774 individuals including their names, phone numbers, email addresses, addresses, date of birth and membership information was compromised.

SCHEDULE B

REMEDIATION PLAN

No.	Remediation action	Status	Target Completion
1	**Vendor relationship management** Starbucks SG will require Ascentis to update Starbucks SG in writing as soon as possible but not later than 21 working days after change has taken effect in changes of their contractors, business structure, which will impact/affect Starbucks SG's services delivery, including any changes in their business structure or any Project Team (roles and responsibilities) movement.	Completed	With immediate effect.
2	Starbucks SG will perform vendor assessment on Ascentis using Starbucks SG's internal Cybersecurity Assessment Form and Vendor Evaluation Form.	Completed	30-Nov-22
3	Starbucks SG will review the audit report after Ascentis performed their own audit on their subcontractors who handle any of Starbucks SG's operations or matters. If any deficiencies noted in relation to any subcontractor, Starbucks SG would require Ascentis to rectify the deficiencies noted in the audit report.	Completed	15 February 2023
4	If the audits conducted in items 2 and 3 above are unsatisfactory, Starbucks SG will require Ascentis to rectify any deficiencies. Thereafter, Starbucks SG will carry out a further security audit on Ascentis to verify that all rectification works have been completed.	In Progress	May 2023
5	Starbucks SG will review Ascentis' ex-employee's compromised account profile for any suspicious activity in the past one year. Starbucks SG will take necessary actions following the discovery of any suspicious activity.	Completed	February 2023
6	Starbucks SG will review Ascentis' processes, and will restrict admin portal access based on IP address.	Completed	27-Sep-22

7	Starbucks SG will set up a virtual private network to connect to and access the admin portal of the e-commerce system.	Completed	27-Sep-22
8	Starbucks SG will require Ascentis to review and improve personal data stored on e-commerce module such that customer data is only stored when strictly necessary. Starbucks SG will further require Ascentis to purge unnecessary account information, review data retention in ecommerce and define retention period. Starbucks SG will carry out follow-up checks to ensure that the above are carried out.	Completed	28-Oct-22
9	Starbucks SG will require Ascentis to implement two-factor authentication to access any admin portal.	In progress	By 30-Apr-23
10	Starbucks SG will require Ascentis to implement customer access geo-restrictions.	Completed	16-Sep-22
11	Starbucks SG will require Ascentis to improve on its processes on monitoring users' activity logs. This includes reviewing existing event monitoring implementation and to look at implementing rule based alerts to manage all logs for automatic anomaly detection and log management.	In Progress	By 31-Mar-23
12	Starbucks SG will require Ascentis to do the following: (a) put in place processes such that Starbucks SG is the gatekeeper/approving party when creating user and removing user in ecommerce admin portal; (b) any Ascentis admin user that is created should be approved by Starbucks SG; (c) where any Ascentis admin user is terminated, Ascentis should promptly inform Starbucks for immediate deprovision; (d) any Starbucks admin user creation and termination will be done and approved by Starbucks IT; and	Completed	16-Sep-22

	(e) review and disable inactive users and shared accounts accessing to e-commerce admin portal.		
13	Starbucks SG will require Ascentis to: (a) review Ascentis' admin portal Role-based Access; (b) review all access rights granted in admin portal, to ensure only required permission granted to approved personnel and roles assigned; and (c) review if the proper rights are given to each role.	Completed	31-Oct-22
14	Starbucks SG will require Ascentis to ensure that the application programming interface is reset (API Access Key) as a precautionary measure.	Completed	19-Sep-22
15	Starbucks SG will review its existing contracts with Ascentis and include relevant data protection clauses that set out clearly the obligations and responsibilities of all parties to comply with PDPA.	In Progress.	By Mid 2023

SCHEDULE C

Case number: DP-2209-C0193

In the matter of an investigation under section 50(1)

of the Personal Data Protection Act 2012 ("the Act")

And

(1) Starbucks Coffee Singapore Pte. Ltd. (UEN No. 198800670D)

… Organisation

DECLARATION

I refer to the voluntary undertaking dated _____ given by the Organisation to the Personal Data Protection Commission pursuant to section 48L of the Act ("**the Undertaking**").

I declare that the remediation plan set out at Schedule B of the Undertaking has been completed.

I acknowledge that by making a false declaration or providing false or misleading information to the Personal Data Protection Commission, I may be prosecuted for offences under section 51(3)(c) of the Personal Data Protection Act 2012 and/or section 182 of the Penal Code 1871.

_____ _____

Signature Date

_____ _____

Name Designation