Monetary Authority of Singapore
10 Shenton Way MAS Building Singapore 079117 Telephone: (65) 6225 5577 Facsimile: (65) 6229 9229

Circular No. ID 03/23

22 February 2023

To Chief Executives
All Insurers

Dear Sir/ Madam

NOTIFICATION OF DATA BREACHES TO THE MONETARY AUTHORITY OF SINGAPORE ("THE AUTHORITY")

Following the issuance of Circular No. ID 10/14 "Notification to the Monetary Authority of Singapore on Events of Significant Impact" on 30 September 2014, the Personal Data Protection (Amendment) Act 2020 came into operation on 1 February 2021, introducing mandatory data breach notification requirements for organisations in Singapore. The Personal Data Protection (Notification of Data Breaches) Regulations 2021 was subsequently issued, and specified the types of data breaches notifiable to the Personal Data Protection Commission ("PDPC").

2 In view of the above-mentioned regulatory developments, the Authority sets out below the revised expectations for licensed insurers regarding the expectations for notifying the Authority of data breaches, as defined under the Personal Data Protection Act 2012. Such data breaches are deemed by the Authority to be events that may have a significant impact on licensed insurers.

(a) The Authority should be concurrently notified of data breaches that are required to be notified to PDPC;

(b) The Authority should be notified of data breaches that meet the criteria under MAS Notice 127 and the Authority's Guidelines on Outsourcing, based on the timelines indicated within these instruments; and

(c) For data breaches that fall outside paragraphs 2(a) and 2(b), the Authority should be notified of them on a consolidated basis, within 3 weeks from the last day of each quarter starting from Q1 2023. The breaches to be included should be those identified during the quarter, regardless of whether the breaches had occurred during or prior to the quarter. The notification should contain, for each data breach, on a best effort basis –

i. a description of the incident and how it was discovered;

ii. an analysis of the root cause of the incident and the key control deficiencies;

iii. an assessment of the impact of the incident (e.g. number of customers affected, financial and non-financial impact);

iv. a description of the remedial measures taken to manage the incident, including the extent of service recovery performed or the insurer's reasons for deciding not to perform service recovery; and

v. a description of the controls to be implemented to prevent occurrence of similar incidents.

Where there are updates to any of the details in paragraph 2(c) after the initial notification of the data breach, these should be provided together with the subsequent quarter's notification to the Authority.

3 This circular supersedes Circular No. ID 10/14 with immediate effect.

4 Please contact your company's liaison officer should you require further clarification.

Yours faithfully

[sent via MASNET]

DANIEL WANG
EXECUTIVE DIRECTOR
INSURANCE DEPARTMENT