Star Health and Allied Insurance Co. Ltd.

Date: October 12, 2024
Place: Chennai

Ref: SHAI/B & S/SE/128/2024-25

To,
BSE Surveillance,
Online Surveillance,
BSE Limited,
Phiroze Jeejeebhoy Towers,
Dalal Street,
Mumbai – 400001.
Maharashtra, India.
Scrip Code: 543412

Sub: **Clarification regarding news item appearing in "Media / Publication".**

Ref:
1. Our intimation bearing reference no. SHAI/B&S/SE/92/2024-25 dated 14 August 2024, issued to the Exchanges.
2. Email from BSE bearing reference L/SURV/ONL/RV/AA/ (2024-2025)/ 74 dated October 11, 2024.

Dear Sir,
With reference to the captioned subject, please find our response below:
Dear Sir,

We, Star Health and Allied Insurance Company Limited (hereinafter, **Star Health** or **We)** write in furtherance of communications referred to above.

We would like to, at the outset, make it known that all of our services remain fully operational without any disruption, and that Star Health has been certified for compliance with the Insurance Regulatory and Development Authority of India (**IRDAI**) Guidelines on Information and Cyber Security of 2023 and with the ISO/IEC 27001 on information security. In addition, Star Health's Board has constituted a Risk Management Committee, which handles the cyber security function.

Background:

As reported on 14 August 2024 to the stock exchanges, Star Health is carrying out an investigation with regard to unauthorized access by an unknown person or group of persons (**Threat Actor** or **TA**) to certain customer data. A thorough investigation by independent cybersecurity experts was immediately initiated and is underway. We have also reported the incident to all relevant regulatory agencies including the Computer Emergency Response Team (**CERT-In**) and the IRDAI on 14 August 2024. Separately, we have filed a Complaint before the Commissioner of Police, Chennai on 14 August 2024 based on which a First Information Report (**FIR**) was registered by the Tamil Nadu Police Cyber Crime Cell on 23 September 2024 reporting the incident, as well as a civil suit on 22 September 2024 before

the Hon'ble Madras High Court, which in its order dated 24 September 2024 has, *inter alia*, directed all third parties, including persons unknown, to disable access to the relevant information. The incident involved a series of emails received by Star Health senior executives, in which the Threat Actor claimed unauthorized and illegal access to the customer confidential data and demanded a ransom amount of USD 68,000. Based on ongoing investigations, the Threat Actor appears to have used bots to purportedly share customer sensitive information through Telegram (the social media and messaging platform) and certain websites.

Immediately after the receipt of emails from the Threat Actor, the circumstances were reported to the Board of Directors which included the members of the Risk Management Committee (RMC), on 14 August 2024. We subsequently initiated necessary and protective steps such as engaging an independent expert to carry out the investigation into the suspected incident, and filing a Police Complaint and intimations to relevant authorities as mentioned above, including the stock exchanges. Regular updates were shared with the Board of Directors on the developments relating to the incident and the investigation, and seeking their guidance on measures to be taken.

We have treated the receipt of ransom-seeking email of 13 August 2024 from the Threat Actor to be a material event as per Regulation 30 of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 (**LODR**) and in compliance of our obligation, have reported the same to the stock exchanges on 14 August 2024. With this context, please see below, our responses.

Responses to Specific Queries:

Query: a) Whether such negotiations were taking place? If so, you are advised to provide the said information along with the sequence of events in chronological order from the start of negotiations till date.

Response: We assume that the query refers to the alleged sale of data by a Star Health executive to a hacker, as mentioned in the Reuters article referred to in your captioned communication (hereafter, **Reuters Article**). We wish to highlight that our investigations are ongoing, and we have engaged competent independent third parties to undertake the exercise. We have not arrived at any finding of wrongdoing by our Chief Information Security Officer (CISO) till date. Once the investigations conclude, we will report the same to the exchanges in accordance with the principles, standards and regulations contained in the LODR, and the Policy for Determination of Materiality for Disclosure of Events or Information as approved by the board of directors and available on our website at https://d28c6jni2fmamz.cloudfront.net/Policy_for_determination_of_materiality_threshold_for_disclosure_of_events_or_information_f770bf0925.pdf.

For your reference, a chronological list of key events pertaining to this matter is set out below:

On 13 August 2024, the Threat Actor demanded a ransom of $68,000 in an email addressed to our MD & CEO from "vladislav rs" (vladislav5533@outlook.com).

Multiple emails were received from the below mentioned email ids:

"vladislav rf" (vladislav5511@outlook.com)

"vladislav rs" (vladislav5533@outlook.com).

Star Health didn't respond to the emails.

14 August 2024: As a responsible insurer, Star Health reported the incident to various relevant authorities as mentioned above.

22 August 2024: TA sent another email on 22 August 2024 and set up a new site called starhealthscam.in. This website was taken down by Star Health. Subsequently, the attacker created yet other websites with the same name, starhealthleak.in, starhealth.lol posting 500 samples of customer data in the website.

29 August 2024: The above websites were taken down by Star Health with help of various law enforcement agencies.

11 September 2024: Star Health issued first notice to Telegram to take down the bots. TA created new bots every time Telegram took down the reported bots. Telegram refused to share the account KYC details or permanently ban the TA's accounts despite multiple notices issued in this regard.

22 September 2024: Plaint filed in Madras High Court against Cloudflare (that is providing certain services to the TA to host the websites), Telegram (where TA hosted bots to disseminate data), unknown persons represented by Ashok Kumar and xenZen (TA) seeking permanent injunction against leaking of Star Health data and misuse of Star Health intellectual property.

23 September 2024: Tamil Nadu Cyber Cell registered the FIR against unknown person based on our complaint under Sections 303 and 308 of Bharatiya Nyaya Sanhita read with Sections 43 and 66 of the Information Technology Act.

24 September 2024: Madras High Court issued ad-interim injunctions restraining anyone from using the Star Health brand and domain names restraining everyone from publishing or making available or continue to make available the data purportedly ex-filtrated from Star Health systems.

Star Health has been making diligent efforts to pursue the implementation of this order since then by notifying the various authorities and third parties.

Query: b) Whether you/company are aware of any information that has not been announced to the Exchanges which could explain the aforesaid movement in the trading? If so, you are advised to provide the said information and the reasons for not disclosing the same to the Exchange earlier as required under Regulation 30 of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015.

Response: The material event, in our view, was the receipt of the emails which was reported by Star Health nearly two months earlier on 14 August 2024 to the relevant authorities, including to the exchanges. The Reuters Article only regurgitated known events previously reported by us, and the change in trading price on 11 October 2024 appears to have occurred as a result of the Reuters Article followed by similar media articles (which, in turn, appear to have taken root from certain third party user posts on the social media platform, 'X') pertaining to the suspected cyber incident, rather than any

specific adverse events occurring on or around that date. This is demonstrated by the fact that Star Health's press statement dated 9 October 2024 containing clarifications were carried in the Reuters Article.

Current Status:

We wish to state that we have taken all measures to secure our systems by exercising additional controls. We have also informed and sought the assistance of the Tamil Nadu Cyber Security Authorities to help us identify the Threat Actor for suitable action.

For the sake of clarity, mentioned below are the Containment, Recovery and Communication Strategies adopted by Star Health to protect the privacy and interests of the Policyholders -

- FIR filed with TN Cyber Police on 23 September 24 against the entities involved in carrying out this incident and investigations are underway. Attached for reference.
- The Honorable High Court of Madras has issued injunction dated 24 September 24 in a civil suit filed by Star Health against Telegram, Cloudflare, XenZen and Unknown Adversaries, *inter alia*, to prevent the leak, dissemination, and sale of sensitive data. Attached for reference.
- A comprehensive independent forensic investigation, led by cybersecurity experts, is in progress and will be concluded before the end of October.
- All identified preventive and proactive measures communicated to concerned stakeholders to contain the incident and further strengthen the information technology (IT) and digital landscape with action plan and timelines.
- Star Health is keeping the regulator IRDAI and its Board of Directors updated on all developments and seeking their guidance.
- Core Crisis Committee working closely with media and regulatory authorities to minimize the reputational impact.
- Star Health has released a media statement on 9 October 2024 providing assurance to our customers.

Any other rumours or reports which are not in line with the above version of events are false and denied.

Please let us know if you have any further queries. We are fully compliant and remain committed to our obligations under the LODR and are available to answer any questions you may have.

Thanking you,
Sincerely,
For Star Health and Allied Insurance Company Limited

JAYASHREE SETHURAMAN

Digitally signed by JAYASHREE SETHURAMAN
Date: 2024.10.12 15:02:00 +05'30'

Jayashree Sethuraman
Company Secretary & Compliance Officer