**1923140**

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:** **Joseph J. Simons, Chairman**
**Noah Joshua Phillips**
**Rohit Chopra**
**Rebecca Kelly Slaughter**
**Christine S. Wilson**

**In the Matter of**

**SKYMED INTERNATIONAL, INC.,**
**also doing business as SkyMed Travel and Car Rental Pro,**
**a Nevada corporation.**

**DOCKET NO.**

## COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that SkyMed International, Inc., a Nevada corporation, has violated the provisions of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent SkyMed International, Inc. ("Respondent"), also doing business as SkyMed Travel and as Car Rental Pro, is a Nevada corporation with its principal office or place of business at 9089 E. Bahia Drive, Suite 100, Scottsdale, Arizona 85260.

2. The acts and practices of Respondent, as alleged in this Complaint, have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

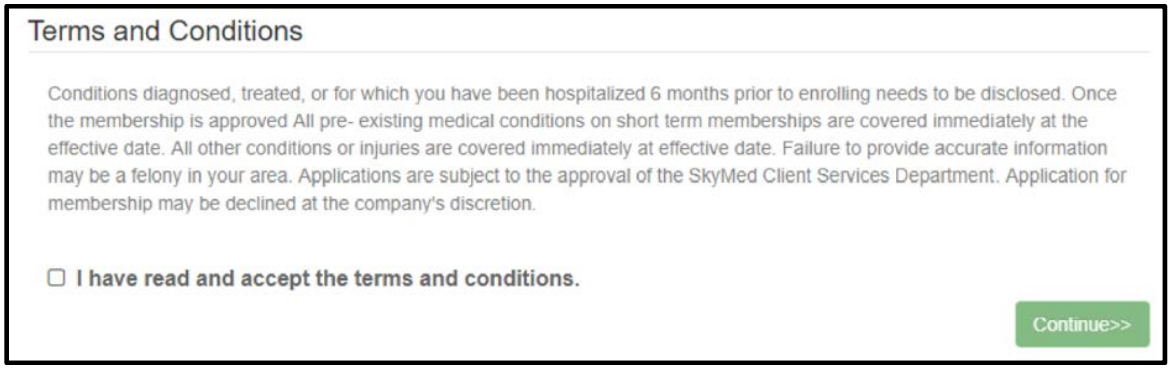
## Respondent's Business Practices

3. Respondent advertises, offers for sale, and sells nationwide a wide array of emergency travel membership plans that cover up to eighteen different emergency travel and medical evacuation services for members who sustain serious illnesses or injuries during travel in certain geographic areas. These services include hospital-to-hospital air transportation, vehicle return, visitor transportation, repatriation for recuperation near home, medical escort flights, and transportation of children.

4. Membership plans provide coverage on a short-term, yearly, or multi-year basis for both single members and entire families. Depending on the term, number of members, and the medical evacuation services covered, membership plans cost between $299 and $8,990.

5. Consumers purchase membership plans through either an online application on Respondent's website or a paper application submitted to an authorized sales representative. In both instances, Respondent collects a significant amount of personal information from applicants, including name, date of birth, sex, home address, email address, phone number, emergency contact information, passport number, and payment card information.

6. Both the online and written applications also mandate that consumers provide Respondent with detailed health information—i.e., a list of prescribed medications and medical conditions, as well as all hospitalizations in the previous six months. Consumers cannot purchase membership plans without providing Respondent this information. In fact, in the online application, Respondent requires that consumers agree to the following terms and conditions:




7. Likewise, the written application includes similar terms and conditions, and applicants must give Respondent express permission to obtain their medical records.

8. Thousands of consumers have signed up for Respondent's membership plans, meaning Respondent has collected a trove of personal information, including sensitive health information, about these consumers.

## Respondent's Deceptive HIPAA Seal

9. Respondent has prominently displayed seals on every page of its website. From 2014 to April 30, 2019, Respondent displayed a seal—in close proximity to two seals provided by third parties—that attested to Respondent's purported compliance with the Health Insurance Portability and Accountability Act ("HIPAA"), a statute that sets forth privacy and information security protections for health data. This seal is circled in red below:


10. By displaying the "HIPAA Compliance" seal on every page of its website, Respondent signaled to consumers that a government agency or other third party had reviewed Respondent's information practices and determined that they met HIPAA's requirements.

11. In reality, no government agency or other third party had reviewed Respondent's information practices for compliance with HIPAA, let alone determined that the practices met the requirements of HIPAA. Respondent has since admitted that the "seal should not have been on the website" and removed the seal from all pages of its website on or around April 30, 2019.

## Respondent's Information Security Practices

12. Respondent has engaged in a number of practices that failed to provide reasonable security for the personal information it collected, including sensitive health information. Among other things, Respondent:

a. failed to develop, implement, or maintain written organizational information security standards, policies, procedures, or practices;

b. failed to provide adequate guidance or training for employees or third-party contractors regarding information security and safeguarding consumers' personal information;

c. stored consumers' personal information on Respondent's network and databases in plain text, without reasonable data access controls or authentication protections;

d. failed to assess the risks to the personal information stored on its network and databases, such as by conducting periodic risk assessments or performing vulnerability and penetration testing of the network and databases;

e. failed to have a policy, procedure, or practice for inventorying and deleting consumers' personal information stored on Respondent's network that is no longer necessary; and

f. failed to use data loss prevention tools to regularly monitor for unauthorized attempts to transfer or exfiltrate consumers' personal information outside of Respondent's network boundaries.

**Respondent's Failure to Secure Consumers' Personal Information**

13. Respondent's failure to provide reasonable security for the personal information it collected led to exposure of some of the information in a cloud database. In March 2019, a security researcher, using a publicly available search engine, discovered an unsecured cloud database maintained by Respondent. According to the security researcher, the database, which could be located and accessed by anyone on the internet, contained approximately 130,000 membership records with consumers' personal information stored in plain text, including information populated in certain fields for names, dates of birth, gender, home addresses, email addresses, phone numbers, membership information and account numbers, and health information (i.e., "hospitalized," "hos_explanation," "prescription," "prescription_list," and "medical").

14. On March 27, 2019, the security researcher notified Respondent about the existence of the database and provided screenshots showing that the database contained consumers' personal information. The security researcher also informed Respondent that anyone could easily alter, download, or even delete the personal information contained therein. In response to the notification, Respondent deleted the database, including the records contained therein.

15. Respondent failed to detect this unsecured and publicly accessible cloud database for more than five months. In fact, before Respondent received the security researcher's notification, Respondent had no idea that the publicly accessible cloud database even existed, let alone that it contained consumers' personal information stored in plain text. Thus, had the exposure not been discovered by the security researcher, it would have continued.

**Respondent's Notification to Consumers Regarding the Security Incident**

16. On May 2, 2019, Respondent notified current and former membership plan holders of this security incident via email. Respondent advised consumers that it had received information from a security researcher about a publicly accessible database containing the consumers' information.

17. Respondent represented that it "immediately took proactive measures to determine the validity of [the security researcher's] allegation, including [by] engaging legal and independent third parties." It also claimed to have investigated the incident, stating:

> Our investigation learned that some old data may have been exposed temporarily as we migrated data from an old system to a new system. At this time, the exposed data has been removed and appears to be limited to only a portion of our information and was restricted to names, street and email addresses, phone and membership ID numbers. **There was no medical or payment-related**

**information visible and no indication that the information has been misused**. (emphasis in original).

18. Multiple consumers responded to Respondent's email notification. Some consumers inquired further about the security incident and the specific personal information exposed, including whether Respondent would be providing identity theft and credit monitoring services. Others requested that Respondent delete all of their personal information. Some consumers praised Respondent for communicating the findings of the investigation into the security incident.

19. Contrary to its representations to consumers described in Paragraph 17, Respondent's investigation did not determine that consumers' health information was neither stored on the cloud database, nor improperly accessed by an unauthorized third party. Rather, Respondent's investigation merely sought to confirm that the database at issue was online and publicly accessible. Upon confirming as much, Respondent immediately deleted the database without ever verifying the types of personal information stored therein. At no point did Respondent examine the actual information stored in the cloud database, identify the consumers placed at risk by the exposure, or look for evidence of other unauthorized access to the database.

## Injury to Consumers

20. Respondent's failure to provide reasonable security for consumers' personal information has caused or is likely to cause substantial injury to those consumers. The information collected by Respondent, including consumers' medical conditions, prescription medications, and previous hospitalizations, together with identifying information such as their names, postal and email addresses, dates of birth, phone numbers, and passport numbers, is highly sensitive. Disclosure of such information, without authorization, is likely to cause stigma, embarrassment, and/or emotional distress. Exposure of this information may also affect a consumer's ability to obtain and/or retain employment, housing, health insurance, or disability insurance. Consumers could lose their jobs, health insurance, or housing if their health information becomes public knowledge.

21. Here, the unsecured cloud database containing more than 130,000 records of consumers' personal information, as described in Paragraph 13, was publicly available on the Internet for at least five months. Due to Respondent's failure to use data loss prevention tools and lack of access controls and authentication protections for its networks, consumers' personal information, including health information, may have been exposed in other instances—beyond the incident described in Paragraphs 13 to 15—without Respondent's knowledge. Even if consumers' personal information had not actually been exposed, Respondent's failure to secure the vast amount of information it has collected has caused or is likely to cause substantial injury to consumers. In particular, health information is valuable on the open market, and wrongdoers frequently seek to purchase consumers' health information on the dark web.

22. The harms described in Paragraphs 20 to 21 were not reasonably avoidable by consumers, as consumers had no way to know about Respondent's information security failures described in Paragraph 12.

23. Respondent could have prevented or mitigated these information security failures through readily available, and relatively low-cost, measures.

## COUNT I – DECEPTION
### HIPAA Seal Misrepresentation

24. Through the means described in Paragraphs 9 and 10, Respondent represented, expressly or by implication, directly or indirectly, that a government agency or other third party had reviewed Respondent's information practices and determined that they met HIPAA's requirements.

25. In truth and fact, as described in Paragraph 11, no government agency or other third party had ever reviewed Respondent's information practices and determined that Respondent's practices met HIPAA's requirements. Therefore, the representation set forth in Paragraph 24 is false or misleading.

## COUNT II – DECEPTION
### Security Incident Response Misrepresentation

26. Through the means described in Paragraph 17, Respondent has represented, directly or indirectly, expressly or by implication, that its investigation into a security researcher's report about an unsecured cloud database determined that consumers' health information was neither stored on the database, nor improperly accessed by an unauthorized third party other than the researcher who reported its exposure.

27. In truth and in fact, as described in Paragraph 19, Respondent's investigation did not determine whether consumers' health information was stored on the cloud database or improperly accessed by an unauthorized third party. Therefore, the representation set forth in Paragraph 26 is false or misleading.

## COUNT III – UNFAIRNESS
### Unfair Information Security Practices

28. Through the means described in Paragraph 12, Respondent failed to employ reasonable measures to protect consumers' personal information, which caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves, as described in Paragraphs 20 to 23. This practice is an unfair act or practice.

## VIOLATIONS OF SECTION 5 OF THE FTC ACT

29. The acts and practices of Respondent, as alleged in this Complaint, constitute unfair and/or deceptive acts or practices, in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this ___ day of ____, 2020, has issued this complaint against Respondent.

By the Commission.

April J. Tabor
Acting Secretary

SEAL: