Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of SkyMed International, Inc.*, File No. 192 3140**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from SkyMed International, Inc., also doing business as SkyMed Travel and Car Rental Pro ("SkyMed").

The proposed consent order ("Proposed Order") has been placed on the public record for thirty days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty days, the Commission again will review the agreement and the comments received, and will decide whether it should withdraw from the agreement or make final the agreement's Proposed Order.

SkyMed is a Nevada corporation with its principal place of business in Arizona. SkyMed provides emergency travel membership plans that cover travel and medical evacuation services for members who sustain serious illnesses or injuries during travel in certain geographic areas. SkyMed has thousands of members. In applying for a membership, a consumer provides his or her name, date of birth, sex, home address, email address, phone number, emergency contact information, passport number, payment card information, a list of prescribed medications and medical conditions, and a list of all hospitalizations in the previous six months.

The Commission's proposed three-count complaint alleges that SkyMed violated Section 5(a) of the Federal Trade Commission Act by engaging in both unfair and deceptive acts or practices.

First, the proposed complaint alleges that SkyMed engaged in a number of unreasonable security practices that led to the exposure of a cloud database containing approximately 130,000 membership records with consumers' personal information stored in plain text. Specifically, the proposed complaint alleges that SkyMed:

- failed to develop, implement, or maintain written organizational information security standards, policies, procedures, or practices;
- failed to provide adequate guidance or training for employees or contractors regarding information security and safeguarding consumers' personal information;
- stored consumers' personal information on SkyMed's network and databases in plain text, without reasonable data access controls or authentication protections;
- 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;
- failed to have a policy, procedure, or practice for inventorying and deleting consumers' personal information stored on SkyMed's network that is no longer necessary; and

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

The proposed complaint alleges SkyMed could have addressed each of these failures by implementing readily available and relatively low-cost security measures.

The proposed complaint alleges that SkyMed's failures caused or are 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. Such practice constitutes an unfair act or practice under Section 5 of the FTC Act.

Second, the proposed complaint alleges that SkyMed engaged in a deceptive act when it notified current and former members about the database exposure. In an email to customers, SkyMed represented that it had investigated the incident and learned that no consumer health information had been exposed in the incident, and that no one had misused the information. In reality, SkyMed did not examine the information stored in the cloud database, identify the consumers placed at risk by the exposure, or look for evidence of unauthorized access to the database. Rather, it merely identified the database and deleted it.

Third, the proposed complaint alleges that SkyMed engaged in a deceptive practice by displaying a seal on every page of its website that attested to its purported compliance with the Health Insurance Portability and Accountability Act, a statute that sets forth privacy and information security protections for health data. SkyMed's display of the seal signaled to consumers that a government agency or other third party had determined that SkyMed's information practices met HIPAA's requirements. The truth is that no government agency or other third party reviewed SkyMed's information practices for compliance with HIPAA, let alone determined that the practices met the requirements of HIPAA.

The Proposed Order contains injunctive relief addressing the alleged unfair and deceptive conduct.

Part I prohibits SkyMed from making false or deceptive statements regarding: (1) the extent to which it is a member of, complies with, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or third party; (2) the extent of any data security incident involving consumers' personal information; (3) the extent of any investigation, and the results thereof, relating to a data security incident; (4) the extent to which SkyMed collects, maintains, uses, discloses, deletes, or permits or denies access to consumers' personal information; and (5) the extent to which SkyMed otherwise protects the privacy, security, availability, confidentiality, or integrity of consumers' personal information.

Part II requires that SkyMed provide notice to all consumers that it previously emailed concerning the database exposure that their personal information, including potentially their health information, may have been exposed in the incident.

Part III requires SkyMed to establish and implement, and thereafter maintain, a comprehensive information security program that protects the security, confidentiality, and integrity of consumers' personal information.

Part IV requires SkyMed to obtain initial and biennial data security assessments for twenty years.

Part V of the Proposed Order requires SkyMed to disclose all material facts to the assessor and prohibits SkyMed from misrepresenting any fact material to the assessments required by Part IV.

Part VI requires SkyMed to submit an annual certification from a senior corporate manager (or senior officer responsible for its information security program) that SkyMed has implemented the requirements of the Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part VII requires SkyMed to notify the Commission any time (1) it is required to make a notification to a federal, state, or local government that personal information has been breached or disclosed, or (2) individually identifiable health information from or about a consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

Parts VIII through XI are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring SkyMed to provide information or documents necessary for the Commission to monitor compliance.

Part XII states that the Proposed Order will remain in effect for twenty years, with certain exceptions.

The purpose of this analysis is to aid public comment on the Proposed Order. It is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify in any way the Proposed Order's terms.