

Complaint

IN THE MATTER OF

SKYMED INTERNATIONAL, INC.**D/B/A****SKYMED TRAVEL AND CAR RENTAL PRO**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT*Docket No. C-4732; File No. 192 3140**Complaint, January 26, 2021 – Decision, January 26, 2021*

This consent order addresses SkyMed International, Inc.’s information security practices and notifications. The complaint alleges that SkyMed violated Section 5 of the Federal Trade Commission Act by using 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. The complaint further alleges that SkyMed engaged in deceptive acts when it notified current and former members about the database exposure, and when displaying a seal on every page of its website that attested to its purported compliance with the Health Insurance Portability and Accountability Act. The consent order 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.

Participants

For the *Commission*: *Brian Berggren* and *Miles Plant*.

For the *Respondents*: *Andrea Bland*, *Russell Duncan*, and *Melissa Ventrone*, *Clark Hill PLC*.

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.

Complaint

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:

Terms and Conditions

Conditions diagnosed, treated, or for which you have been hospitalized 6 months prior to enrolling needs to be disclosed. Once the membership is approved All pre- existing medical conditions on short term memberships are covered immediately at the effective date. All other conditions or injuries are covered immediately at effective date. Failure to provide accurate information may be a felony in your area. Applications are subject to the approval of the SkyMed Client Services Department. Application for membership may be declined at the company's discretion.

☐ I have read and accept the terms and conditions.

Continue>>

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.

Complaint

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;

Complaint

- 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.

Complaint

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

Complaint

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.

Decision and Order

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 twenty-sixth day of January, 2021, has issued this complaint against Respondent.

By the Commission.

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

Respondent and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: (1) statements by Respondent that it neither admits nor denies any of the allegations in the draft Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and (2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of thirty (30) days for the receipt and consideration

Decision and Order

of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondent is SkyMed International, Inc., also doing business as SkyMed Travel and as Car Rental Pro, a corporation with its principal office or place of business at 9089 E. Bahia Drive, Suite 100, Scottsdale, AZ 85260.
2. The Commission has jurisdiction over the subject matter of this proceeding and over Respondent, and the proceeding is in the public interest.

ORDER**Definitions**

For purposes of this Order, the following definitions apply:

- A. “Affected Consumers” means all consumers that received an email from Respondent on or around May 2, 2019 with the subject line, “IMPORTANT MESSAGE relative to SkyMed data exposure.”
- B. “Covered Incident” means any instance in which (a) any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization; or (b) individually identifiable Health Information from or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.
- C. “Health Information” means information relating to the health of an individual consumer, including but not limited to medical history information, prescription information, hospitalization information, clinical laboratory testing information, health insurance information, or physician exam notes.
- D. “Personal Information” means individually identifiable information from or about an individual consumer, including: (a) a first and last name; (b) a home or physical address, including street name and name of city or town; (c) an email address or other online contact information; (d) a mobile or other telephone number; (e) a date of birth; (f) a government-issued identification number, such as a driver’s license, military identification, passport, or Social Security number, or other personal identification number; (g) credit card or other financial account

Decision and Order

information; (h) Health Information; or (i) user account credentials, such as a login name and password.

- E. “Respondent” means SkyMed International, Inc., its successors and assigns, and Global Emergency Travel Services, and its successors and assigns.

Provisions**I. Prohibition Against Misrepresentations**

IT IS ORDERED that Respondent; Respondent’s officers, agents, employees, and attorneys; and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, must not misrepresent in any manner, expressly or by implication:

- A. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any third party, including any self-regulatory or standard-setting organization;
- B. The extent of any Covered Incident or unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of Personal Information;
- C. The extent of any investigation and the results thereof, whether conducted by Respondent, a governmental agency, or a third party, into any Covered Incident or unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of Personal Information;
- D. The extent to which Respondent collects, maintains, uses, discloses, deletes, or permits or denies access to any Personal Information; and
- E. The extent to which Respondent otherwise protects the privacy, security, availability, confidentiality, or integrity of any Personal Information.

II. Required Notice to Consumers About Respondent’s Security Incident Response

IT IS FURTHER ORDERED that, within fourteen (14) days after the effective date of this Order, Respondent must directly notify all Affected Consumers by sending an email, consisting solely of an exact copy of the notice attached hereto as Exhibit A (“Notice”), with the subject line “Update: May 2019 Data Exposure.” Respondent shall not include with the Notice any other information, documents, or attachments.

III. Mandated Information Security Program

IT IS FURTHER ORDERED that Respondent, in connection with the collection, maintenance, use, disclosure, or provision of access to Personal Information, must, within thirty

Decision and Order

(30) days of issuance of this Order, establish and implement, and thereafter maintain, a comprehensive Information Security Program (“Information Security Program”) that protects the security, confidentiality, and integrity of Personal Information. To satisfy this requirement, Respondent must, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Information Security Program;
- B. Provide the written program and any evaluations thereof or updates thereto to Respondent’s board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for Respondent’s Information Security Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;
- C. Designate a qualified employee or employees to coordinate and be responsible for the Information Security Program;
- D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the (1) unauthorized collection, maintenance, use, disclosure of, or provision of access to, Personal Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information;
- E. Design, implement, maintain, and document safeguards that control for the internal and external risks Respondent identifies to the security, confidentiality, or integrity of Personal Information identified in response to sub-Provision III.D. Each safeguard must be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, disclosure of, or provision of access to, Personal Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information. Such safeguards must also include:
 - 1. Policies, procedures, and technical measures to systematically inventory Personal Information in Respondent’s control and delete Personal Information that is no longer necessary;
 - 2. Policies, procedures, and technical measures to log and monitor access to repositories of Personal Information in Respondent’s control;
 - 3. Encryption of, at a minimum, all passport numbers, financial account information, and Health Information in Respondent’s control.
 - 4. Training of all of Respondent’s employees, at least once every twelve (12) months, on how to safeguard Personal Information;

Decision and Order

5. Technical measures to monitor all of Respondent's networks, including all systems and assets within those networks, to identify data security events, including unauthorized attempts to exfiltrate Personal Information from those networks; and
 6. Data access controls for all repositories of Personal Information in Respondent's control, such as (a) restricting inbound connections to approved IP addresses, (b) requiring authentication to access them, and (c) limiting employee access to what is needed to perform that employee's job function.
- F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results;
- G. Test and monitor the effectiveness of the safeguards in place at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and modify the Information Security Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of Respondent's network once every four (4) months and promptly (not to exceed thirty (30) days) after a Covered Incident, and (2) periodic penetration testing of Respondent's network and promptly (not to exceed thirty (30) days) after a Covered Incident;
- H. Select and retain service providers capable of safeguarding Personal Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards for Personal Information; and
- I. Evaluate and adjust the Information Security Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Information Security Program. At a minimum, Respondent must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

IV. Information Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision III of this Order, titled Mandated Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

- A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Information

Decision and Order

Security Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney client privilege, statutory exemption, or any similar claim.

- B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, who the Associate Director shall have the authority to approve in his sole discretion.
- C. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.
- D. Each Assessment must, for the entire assessment period:
 - 1. determine whether Respondent has implemented and maintained the Information Security Program required by Provision III;
 - 2. assess the effectiveness of Respondent's implementation and maintenance of sub- Provisions III.A-I;
 - 3. identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program;
 - 4. address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and
 - 5. identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely solely on assertions or attestations by Respondent's management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent Respondent revises, updates, or adds one or more safeguards

Decision and Order

required under Provision III in the middle of an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

- E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, “In re SkyMed International, FTC File No. 1923140.” All subsequent biennial Assessments must be retained by Respondent until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

V. Cooperation with Third-Party Information Security Assessor

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with any Assessment required by Provision IV must:

- A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;
- B. Provide or otherwise make available to the Assessor information about Respondent’s networks and all of Respondent’s IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the networks and IT assets deemed in scope; and
- C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor’s: (1) determination of whether Respondent has implemented and maintained the Information Security Program required by Provision III; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions III.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

VI. Annual Certification

IT IS FURTHER ORDERED that Respondent must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no

Decision and Order

such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's Information Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents that Respondent verified or confirmed during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re SkyMed International, FTC File No. 1923140."

VII. Covered Incident Reports

IT IS FURTHER ORDERED that Respondent, within thirty (30) days after Respondent's discovery of a Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;
- C. A description of each type of information that was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;
- D. The number of consumers whose information triggered any notification obligation to the U.S. federal, state, or local government entity;
- E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of each materially different notice sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by

Decision and Order

overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re SkyMed International, FTC File No. 1923140."

VIII. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For twenty (20) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order, and all agents, and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in Provision IX. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

IX. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

- A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (1) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (2) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describe the activities of each business, including the goods and services offered, what Personal Information is collected, and the means of advertising, marketing, and sales; (4) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes that Respondent made to comply with the Order; and (5) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

Decision and Order

- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; or (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, “In re SkyMed International, FTC File No. 1923140.”

X. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;
- B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name, addresses, telephone numbers, job title or position, dates of service, and (if applicable) the reason for termination;
- C. Copies or records of all consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;
- D. A copy of each unique advertisement or other marketing material making a representation subject to this Order;

Decision and Order

- E. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, security, availability, confidentiality, or integrity of any Personal Information, including any representation concerning a change in any website or other service controlled by Respondent that relates to privacy, security, availability, confidentiality, or integrity of Personal Information;
- F. For five (5) years after the date of preparation of each Assessment required by this Order, all materials and evidence that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;
- G. For five (5) years from the date received, copies of all subpoenas and other communications with law enforcement, if such communications relate to Respondent's compliance with this Order;
- H. For five (5) years from the date created or received, all records, whether prepared by or on behalf of Respondent, that tend to show any lack of compliance by Respondent with this Order; and
- I. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

XI. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within ten (10) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the

Decision and Order

Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XII. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance, (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than twenty (20) years;
- B. This Order's application to any Respondent that is not named as a defendant in such complaint; and
- C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Exhibit A

[To appear with the SkyMed logo]

Dear [Customer]:

In May 2019, we notified you by email that your personal information saved in a SkyMed database was exposed between October 2018 and March 2019. We said that there was no evidence that anyone had misused it. We also said that your health information and your financial information were not exposed.

Analysis to Aid Public Comment

We have since learned that the exposed database may have contained some members' health information, possibly including yours, and which may have included whether you were hospitalized or took any prescription medications. In addition, the other personal information exposed in the database included:

- your name
- your mailing address
- your email address
- your date of birth
- your phone number
- your membership number

Your Social Security number was not exposed. Neither was your financial information.

We've since put in place a new information security program to protect your information. If you have any questions or comments about this data exposure or what we do to protect your information, please contact us at [[email address]].

Eleanore Klein
President, SkyMed Group of Companies

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

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.

Analysis to Aid Public Comment

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,

Analysis to Aid Public Comment

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.

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

**BIONATROL HEALTH, LLC,
ISLE REVIVE, LLC d/B/A ISLE REVIVE CBD,
MARCELO TORRE,
AND
ANTHONY MCCABE**

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTIONS 5 AND 12 OF THE
FEDERAL TRADE COMMISSION ACT

Docket No. C-4733; File No. 202 3114

Complaint, January 28, 2021 – Decision, January 28, 2021

This consent order addresses Bionatrol Health, LLC's advertising for products containing cannabidiol, including Bionatrol Full-Spectrum CBD Oil Extract. The complaint alleges that Respondents violated Sections 5(a) and 12 of the Federal Trade Commission Act by disseminating false and unsubstantiated advertisements claiming that their CBD Products, among other things: are safe for all users; treat pain better than prescription medicine like OxyContin; prevent and treat age-related cognitive decline, chronic pain, including arthritis pain, heart disease, hypertension, and migraines; and are "medically proven" to (a) improve anxiety, insomnia, chronic pain, hypertension, and cardiovascular health; (b) treat depression and bipolar disorder; (c) reduce age-related cognitive decline; (d) improve memory recall; and (e) reduce arthritis pain, migraines, and headaches. The complaint further alleges that Respondents misrepresented the cost to purchase one bottle of their CBD Oil Extract and unfairly charged consumers' credit cards for the additional cost without their express informed consent. The consent order prohibits Respondents from making any representation about the efficacy of any covered product, unless the representation is non-misleading, including that, at the time such representation is made, they possess and rely upon competent and reliable scientific evidence that substantiates that the representation is true.

Participants

For the *Commission*: Keith Fentonmiller.

For the *Respondents*: Karl Kronenberger, Kronenberger Rosenfeld, LLP.

COMPLAINT

The Federal Trade Commission, having reason to believe that Bionatrol Health, LLC, a corporation, Isle Revive, LLC, also d/b/a Isle Revive CBD, a corporation, Marcelo Torre, individually and as an owner and manager of Bionatrol Health, LLC and Isle Revive, LLC, and Anthony McCabe (collectively, "Respondents"), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Bionatrol Health, LLC ("Bionatrol") is a Utah corporation with its principal place of business at 1269 W. Spencer Rd., Pleasant Grove, Utah 84062. Bionatrol's business registration with the State of Utah expired on May 14, 2020.