1923140

UNITED STATES OF AMERICA

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

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.

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

By the Commission.

April J. Tabor
Acting Secretary

SEAL: