

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 21-071

**Investigation by LETITIA JAMES,
Attorney General of the State of New York, of**

EYEMED VISION CARE LLC,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (“NYAG”) commenced an investigation pursuant to, *inter alia*, Executive Law § 63(12) and General Business Law (“GBL”) §§ 349 and 899-bb into a data security incident at EyeMed Vision Care LLC (“EyeMed” or “Respondent”). This Assurance of Discontinuance (“Assurance”) contains the findings of NYAG’s investigation and the relief agreed to by NYAG and EyeMed.

NYAG FINDINGS

1. On or about June 24, 2020, unknown attacker(s) (the “attacker”) gained access to an EyeMed email account, used by some EyeMed Clients¹ to provide sensitive consumer data in connection with vision benefits enrollment and coverage, when the attacker entered login credentials via a web browser and mail client.

¹ EyeMed is in the business of making vision benefits available to individuals who are members of (1) fully insured vision benefit plans offered by licensed underwriters and (2) self-funded plans offered by employers. In doing so, EyeMed contracts with the underwriters and employers (collectively, “EyeMed Clients”) to offer services to the individual members.

2. The intrusion, which lasted approximately a week, granted the attacker access to, and the ability to view, emails and attachments dating back six years prior to the attack. Those emails contained one or more of the following consumer data elements: names; contact information including addresses; dates of birth; account information including identification numbers for health insurance accounts and vision insurance accounts; full or partial Social Security Numbers; Medicaid numbers, Medicare numbers, drivers license or other government ID numbers, birth or marriage certificates, medical diagnoses and conditions, and medical treatment information. Not every data element was impacted for every individual. In total, information for approximately 2.1 million individuals was exposed, including approximately 98,632 New Yorkers.

3. EyeMed did not detect the unauthorized access to the email account at the time it occurred.

4. From June 24 through July 1, 2020, the attacker accessed the email account from a number of IP addresses, some of which were outside of the United States.

5. On July 1, 2020, the attacker sent approximately 2,000 phishing emails from the enrollment email account to EyeMed Clients. The phishing messages purported to be a request for proposal to deceive recipients into providing credentials to the attacker. Later the same day, EyeMed's IT department observed the transmission of these phishing emails from the email account, and received inquiries from clients about the suspicious emails. EyeMed blocked the attacker's access to the email account, and EyeMed's internal IT team began investigating the scope of the incident.

6. After its internal investigation, from approximately July 14 through July 19, 2020, EyeMed engaged a leading forensic cybersecurity firm through outside counsel to conduct a

forensic investigation. The investigation confirmed that the attacker had the ability to exfiltrate the documents and information within the affected email account during the time that the attacker was accessing the account. Investigators were unable to rule out that such exfiltration had occurred.

7. Following review of the documents in the impacted mailbox by a leading document review vendor, beginning September 28, 2020, EyeMed began to notify affected individuals and regulators about the breach. Notification of affected individuals continued on a rolling basis, following receipt of direction from EyeMed Clients, through January 28, 2021. EyeMed offered affected individuals complimentary credit monitoring, fraud consultation, identity theft restoration. For affected minors, EyeMed offered Minor Social Security Number trace, fraud consultation, and identity theft restoration services.

8. The NYAG's investigation identified the following areas where EyeMed's practices did not meet the requirements of General Business Law § 899-bb to protect customer personal information:

- a. Authentication: EyeMed failed to implement multifactor authentication ("MFA") for the affected email account, despite the fact that the account was accessible via a web browser and contained a large volume of consumers' sensitive personal information. EyeMed was aware of the importance of MFA to reasonable data protections, having required MFA for years before the attack for users to access EyeMed's VPN.²
- b. Password Management: EyeMed failed to use sufficient password management

² EyeMed had begun to roll out MFA to email accounts before the attack occurred; however, EyeMed failed to apply MFA to the enrollment account in time to prevent the attack. EyeMed completed its rollout of MFA to all email accounts by September 2020.

requirements for the enrollment email account given that it was accessible via a web browser and contained a large volume of sensitive personal information. EyeMed set a minimum password length of only eight characters for the affected email account. The password that the attacker used to gain access to the account was insufficiently complex given the sensitivity of the information in the enrollment account. At the time of the attack, EyeMed was aware of the importance of password complexity to reasonable data protections, having required passwords to be at least twelve characters long for accounts with elevated privileges, such as administrator accounts. Additionally, at the time of the attack, EyeMed permitted six failed login attempts before locking out the user ID.³

- c. Logging & Monitoring: EyeMed failed to maintain adequate logging and monitoring of its email accounts, making it difficult to investigate security incidents. At the time of the attack, EyeMed used an Office 365 E3 license for the email account, which provided limited logging capabilities and did not allow recording of logs for longer than 90 days or permit visibility into an individual's activities within the email account mailbox. Thus, EyeMed was unable to see when mail items were accessed; when mail items were replied to or forwarded beyond 90 days; or identify when a user searched and what the user searched for. As a result, the forensic cybersecurity firm was unable to

³ After the attack, EyeMed decreased the number of login attempts that could be attempted unsuccessfully before an account was locked out.

definitively determine what emails or documents were accessed by the unauthorized user.⁴

- d. Data Retention in the Affected Email Account: The breach included customer information from six years prior to the breach because the email account was used by some EyeMed Clients to make changes in vision coverage and it contained emails with consumer's personal information dating back to January 3, 2014. It was unreasonable to leave personal information in the affected email account for up to six years rather than to copy and store such information in more secure systems and delete the older messages from the affected email account, particularly in light of the unreasonable protections for the affected email account at the time of the breach as detailed in subparagraphs 8.a-8.c above.

9. EyeMed's online privacy policy contains the following representation to consumers:

The security of your personal information^[5] is important to us. We follow generally accepted industry standards to protect the personal information submitted to us, and to guard that information against loss, misuse or alteration. When you enter personal information on our Site, we encrypt transmissions involving such information using secure protocols.

10. Based on the foregoing, EyeMed violated Executive Law § 63(12), GBL §§ 349 and 899-bb.

11. Respondent neither admits nor denies NYAG's Findings, paragraphs 1-10 above.

⁴ After the attack, EyeMed obtained an Office 365 E5 license, which provides improved logging capabilities, including the ability to retain audit logs for up to one year and the ability to identify when mail items were accessed.

⁵ EyeMed's online privacy policy defines "personal information" broadly to include information "such as your name, contact information, or information about your company."

12. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12) and GBL §§ 349 and 899-bb.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

PROSPECTIVE RELIEF

13. For the purposes of this Assurance, the following definitions shall apply:
- A. “Affected Consumer” shall mean any person whose Personal Information was subject to the Security Event.
 - B. “Credit Report” shall mean consumer report as defined in 15 U.S.C. § 1681a(d), and any amendments thereto.
 - C. “Effective Date” shall be the date of the last signature to this agreement.
 - D. “Personal Information” shall mean information provided by a customer that can be used to identify a customer, or about a customer, including name, home or other physical address, email address, Social Security number, government ID number including driver's license number, bank account number, credit or debit card number, medical or health insurance information, medical diagnostic information, photographic image, fingerprints, handwriting or other unique biometric data, or information defined as private information in GBL § 899-aa.

- E. “Security Event” shall mean any compromise that results in unauthorized access to or acquisition of Personal Information owned, licensed, or maintained by EyeMed.

GENERAL COMPLIANCE

14. EyeMed shall comply with Executive Law § 63(12), and GBL §§ 349 and 899-bb, in connection with its collection, use, and maintenance of Personal Information, and shall maintain reasonable security policies and procedures designed to safeguard Personal Information from unauthorized use or disclosure.

15. EyeMed shall not misrepresent the extent to which EyeMed maintains and protects the privacy, security, confidentiality, or integrity of Personal Information collected from or about customers.

INFORMATION SECURITY PROGRAM

16. EyeMed shall maintain a written information security program (“Information Security Program”) that is reasonably designed to protect the security, integrity, and confidentiality of Personal Information that EyeMed collects, stores, transmits, and/or maintains. The Information Security Program shall, at a minimum, include the information security requirements set forth in this Assurance.

17. The Information Security Program shall comply with applicable requirements under New York state law, including General Business Law §§ 899-bb, and shall contain reasonable administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of EyeMed’s operations; (ii) the nature and scope of EyeMed’s activities; and (iii) the sensitivity of the Personal Information that EyeMed collects, stores, transmits, and/or maintains.

18. EyeMed shall review the Information Security Program not less than annually and make any reasonable changes necessary to ensure the protection of the security, integrity, and confidentiality of Personal Information that EyeMed collects, stores, transmits, and/or maintains.

19. EyeMed shall employ a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program with the credentials, background, and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program.

20. EyeMed shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program. EyeMed shall provide the training required under this paragraph to such employees within thirty (30) days of the Effective Date of this Assurance or prior to their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

PERSONAL INFORMATION SAFEGUARDS AND CONTROLS

21. Password Management: EyeMed shall maintain reasonable password policies and procedures requiring the use of complex passwords, and ensuring that stored passwords are properly protected from unauthorized access, including, without limitation, hashing stored passwords using a reasonable hashing algorithm and salting policy commensurate with security risks that are known or reasonably should be known.

22. Authentication Policy and Procedures: EyeMed shall maintain reasonable account management and authentication, including forbidding the use of shared user accounts, requiring passwords to be changed at least every 90 days, and requiring the use of multi-factor authentication for all administrative or remote access accounts. It shall be evaluated on an annual basis for

ensuring its adequacy and relevancy regarding EyeMed's needs and goals.

23. Encryption: EyeMed shall encrypt customer Private Information as defined by GBL § 899-aa(b) that it collects, stores, transmits and/or maintains, whether stored within the EyeMed computer network, or transmitted electronically within or outside the network, using a reasonable encryption algorithm where technically feasible.

24. Penetration Testing: EyeMed shall maintain a reasonable penetration testing program designed to identify, assess, and remediate security vulnerabilities within the EyeMed computer network. This program shall include regular penetration testing, risk-based vulnerability ratings, and vulnerability remediation practices that are consistent with industry standards.

25. Logging and Monitoring: EyeMed shall implement and maintain an appropriate system designed to collect and monitor network activity, such as through the use of security and event management tools, as well as appropriate policies and procedures designed to properly configure such tools to report anomalous activity. Logs for network activity should be actively accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

26. Data Deletion: EyeMed shall permanently delete customer Personal Information when there is no reasonable business or legal purpose to retain it.

27. EyeMed shall continue to provide Affected Consumers who enrolled in the following identified monitoring services with those services at no cost for an aggregate of two (2) years:

- a. Credit Monitoring: Daily Credit Report monitoring from a nationwide consumer reporting agency (i.e., Equifax Information Services LLC, Experian

Information Solutions, Inc., or TransUnion LLC) showing key changes to an Affected Consumer's Credit Report including automated alerts where the following occur: new accounts are opened; inquiries or requests for an Affected Consumer's Credit Report for the purpose of obtaining credit; changes to an Affected Consumer's address; and negative information, such as delinquencies or bankruptcies.

- b. Fraud Consultation and Identity Theft Restoration: provide live support and explanation of the identity theft restoration process to ensure the victim understands his or her rights and responsibilities; investigate and resolve complicated trails of fraudulent activity; issue fraud alerts for the victim with the three consumer credit reporting agencies, the Social Security Administration, the Federal Trade Commission and the U.S. Postal Service; prepare appropriate documentation, from dispute letters to defensible complaints; work all identity theft issues until they have been verifiably resolved with all the organizations impacted including financial institutions, collections agencies, check clearinghouse companies, landlords, property managers, and government entities; and
- c. Social Security Number trace for minors.

28. EyeMed shall pay to the State of New York Six Hundred Thousand Dollars (\$600,000). Payment shall be made payable to the State of New York in full within forty-five (45) days of the Effective Date of this Assurance. Any payment shall reference AOD No. 21-071.

29. The Respondent shall provide NYAG with a certification affirming its compliance

with the requirements set forth in this Assurance, paragraphs 14-26, to be submitted to NYAG within sixty (60) days of the Effective Date of this Assurance. This certification shall be in writing and be signed by an officer of Respondent. Thereafter, a certification of compliance shall be submitted to NYAG on an annual basis for the following three (3) years. In any case where the circumstances warrant, NYAG may require Respondent to file an interim certification of compliance upon thirty (30) days notice.

MISCELLANEOUS

30. Respondent expressly agrees and acknowledges that NYAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 37, and agrees and acknowledges that in the event the Assurance is voided:

- a. any statute of limitations or other time-related defenses are tolled from and after the Effective Date of this Assurance;
- b. the NYAG may use statements, documents or other materials produced or provided by Respondent prior to or after the Effective Date of this Assurance;
- c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue; and
- d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

31. If a court of competent jurisdiction determines that Respondent has violated the Assurance, Respondent shall pay to the NYAG the reasonable cost, if any, of obtaining such

determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

32. This Assurance (including without limitation any and all legal and factual statements herein) is not intended to be and shall not in any event be construed or deemed to be, or represented or caused to be represented as, an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of EyeMed or of any fact or violation of any law, rule, or regulation. This Assurance is made without trial or adjudication of any alleged issue of fact or law and without any finding of liability of any kind. This Assurance is not intended for use by any third party in any other proceeding.

33. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Respondent. Respondent shall include in any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of NYAG.

34. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

35. Any failure by the NYAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the NYAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by Respondent.

36. All notices, reports, requests, and other communications pursuant to this Assurance

must reference Assurance No. 21-071, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Respondent, to:

Thora Johnson
Orrick, Herrington & Sutcliffe
Columbia Center
1152 15th Street, NW
Washington, DC 20005
Thora.Johnson@Orrick.com

If to NYAG, to:

Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005

37. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondent and its counsel and NYAG's own factual investigation as set forth in NYAG's Findings, paragraphs 1-10 above. Respondent represents and warrants that neither it nor its counsel has made any material misrepresentations to NYAG. If any material misrepresentations by Respondent or its counsel are later found to have been made by NYAG, this Assurance is voidable by NYAG in its sole discretion.

38. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondent in agreeing to this Assurance.

39. Respondent represents and warrants, through the signature below, that the terms

and conditions of this Assurance are duly approved.

40. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

41. Nothing contained herein shall be construed to limit the remedies available to NYAG in the event that Respondent violates the Assurance after its Effective Date.

42. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

43. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

44. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.



45. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

46. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

47. This Assurance may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement binding upon all Parties, notwithstanding that all Parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the Effective Date of this Assurance. For purposes of this Assurance, copies of signatures shall

be treated the same as originals.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance
have been affixed hereto on the dates set forth below.

<p>LETITIA JAMES ATTORNEY GENERAL OF THE STATE OF NEW YORK</p> <p>By: <u></u> Noah Stein Assistant Attorney General Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005</p> <p><u>1/18/2022</u> Date</p>	<p>EYEMED VISION CARE LLC</p> <p>By: <u></u> Emilia Flamini Chief Financial Officer EyeMed Vision Care LLC 4000 Luxottica Place Mason, OH 45040</p> <p><u>1/11/2022</u> Date</p>
--	---