

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street, 5th Floor
P.O. Box 45029
Newark, New Jersey 07101
Attorney for the New Jersey Division of Consumer Affairs

FILED

May 16 2023

Division of Consumer Affairs

By: Gina F. Pittore
Deputy Attorney General
(973) 648- 4137

In the Matter

EyeMed Vision Care LLC,

Respondent.

ASSURANCE OF VOLUNTARY
COMPLIANCE

WHEREAS this matter having been opened by the Attorneys General of Oregon, New Jersey, Florida, and Pennsylvania (collectively, “Attorneys General”) as an investigation to ascertain whether violations of the Consumer Protection Acts, Personal Information Protection Acts, as defined below, and/or the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 to 180 (collectively, “HIPAA”) have been or are being committed (the “Investigation”) by EyeMed Vision Care LLC, its wholly owned, integrated, and operated subsidiaries and divisions, successors, and assigns, officers, Executive Staff, and employees doing business in the United States (“EyeMed”).

WHEREAS the Attorneys General are charged with the responsibility of enforcing the Consumer Protection Acts and Personal Information Protection Acts;

WHEREAS the Attorneys General may, pursuant to 42 U.S.C. § 1320d-5(d), enforce the provisions of HIPAA;

WHEREAS the Attorneys General allege that EyeMed engaged in conduct that violated the Consumer Protection Acts, Personal Information Protection Acts, and HIPAA in connection with Personal Information and Protected Health Information.

WHEREAS the Attorneys General and EyeMed (collectively, the “Parties”) have reached an amicable agreement resolving the issues in controversy and concluding the Investigation without the need for further action, and EyeMed having cooperated with the Investigation and consented to the entry of the within order (“Agreement”) without admitting any violation of law, and for good cause shown;

IT IS ORDERED AND AGREED as follows:

1. EFFECTIVE DATE

1.1. This Agreement is effective on June 16, 2023 (“Effective Date”).

2. DEFINITIONS

Unless otherwise defined herein, the following words or terms shall have the following meanings for purposes of this Agreement:

2.1. “Affected Consumers” shall refer to the individuals with PI or PHI potentially impacted by the Breach.

2.2. “Breach” shall refer to the Security Incident, and all events related thereto, discovered by EyeMed on July 1, 2020.

2.3. “Breach Notification Rule” shall refer to 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and D.

2.4. “Business Associate” shall be defined in accordance with 45 C.F.R. § 160.103.

- 2.5. “Consumer Protection Acts” shall mean the State citations listed in Appendix A.
- 2.6. “Covered Entity” shall be defined in accordance with 45 C.F.R. § 160.103.
- 2.7. “Covered Systems” shall mean components, such as servers, workstations, and devices, within the EyeMed Network that are routinely used to collect, process, communicate, and/or store PI and/or PHI.
- 2.8. “Cyber Security Operations Center” or “C-SOC” shall mean the employment of person(s), processes, and technology to continuously monitor EyeMed’s security posture while detecting, analyzing, and responding to Security Incidents.
- 2.9. “Executive Staff” shall mean the following EyeMed employees: President; Chief Financial Officer - North America; Senior Vice President, Sales & Account Management; Vice President, Product Development; Vice President, Sales; Vice President & Secretary; and Assistant Secretary, or the functional equivalents of each position throughout the duration of EyeMed’s business operations within the States.
- 2.10. “EyeMed Email Account” refers to the EyeMed email account compromised during the Breach.
- 2.11. “EyeMed Network” shall mean the networking equipment, databases or data stores, applications, servers, workstations, and endpoints owned and/or operated by EyeMed, which are capable of using and sharing software, data, and hardware resources.
- 2.12. “Minimum Necessary Standard” shall refer to the requirements of the Privacy Rule that, when using or disclosing PHI or when requesting PHI from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d)(1)-(5).

2.13. “Multi-factor Authentication” shall mean user account authentication through verification of at least two of the following factors: (i) knowledge factors such as a password; or (ii) possession factors, such as a token, connection through a known authenticated source, or a text message on a mobile phone; or (iii) inherent factors, such as biometric characteristics.

2.14. “Personal Information” or “PI” shall mean the data elements in the definition of personal information set forth in the Consumer Protection Acts, the Personal Information Protection Acts, and the State Breach Notification Acts.

2.15. “Personal Information Protection Act” shall mean the State citations listed in Appendix B.

2.16. “Privacy Rule” shall refer to 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

2.17. “Protected Health Information” or “PHI” shall be defined in accordance with 45 C.F.R. § 160.103 and includes Electronic Protected Health Information.

2.18. “Security Event” shall mean any compromise by unauthorized access or inadvertent disclosure to the confidentiality, integrity, or availability of PI or PHI of at least 500 United States consumers held or stored within the EyeMed Network.

2.19. “Security Incident” shall be defined in accordance with 45 C.F.R. § 164.304.

2.20. “Security Rule” shall refer to 45 C.F.R Part 160 and 45 C.F.R Part 164, Subparts A and C.

2.21. “State Breach Notification Acts” shall mean the State citations listed in Appendix B.

3. ATTORNEYS GENERAL'S FINDINGS

3.1. EyeMed offers a preferred provider vision network in the U.S.

3.2. EyeMed makes its preferred provider vision network available to members of fully insured vision benefit plans (“Policies”) offered by licensed underwriters (“Issuers”) who have contracted with EyeMed. Each Issuer is a HIPAA Covered Entity, and EyeMed is the Issuer’s Business Associate.

3.3. On behalf of certain Issuers, EyeMed markets the Policies to employer groups. The other Issuers conduct their own marketing (“Resellers”).

3.4. EyeMed also makes its preferred provider vision network available to members of self-funded vision benefit plans offered by employers (“ASO Group Plan”). Each ASO Group Plan is a Covered Entity and EyeMed is the plan’s Business Associate.

3.5. A Reseller may directly contract with the employer group. In these instances, the ASO Group Plan is still the Covered Entity, but the Reseller is the Business Associate and EyeMed is the sub-Business Associate.

3.6. At all relevant times, EyeMed was and continues to be a Business Associate within the meaning of HIPAA.

3.7. As a Business Associate, EyeMed is required to comply with the standards, as applicable, set forth by HIPAA that govern the privacy of PHI, including the Privacy Rule, Security Rule, and Breach Notification Rule.

3.8. On June 24, 2020, at least one unauthorized individual gained access to the EyeMed Email Account, which was used internally and by some EyeMed group clients to communicate, for example, vision care enrollment updates.

3.9. From June 24, 2020, to July 1, 2020, the unauthorized individual(s) accessed the EyeMed Email Account via web browser and mail client by using the EyeMed Email Account login username and password. From June 24, 2020, to July 1, 2020, the unauthorized individual(s) had access into the EyeMed Email Account, which contained emails and attachments dating back six years prior to the attack. The emails contained the one or more of the following PI and PHI from approximately 2.1 million individuals: 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, driver's license or other government identification numbers, birth or marriage certificates, medical diagnoses and conditions, and medical treatment information.

3.10. EyeMed asserts the following:

3.10.1. On July 1, 2020, the attacker sent approximately 2,000 phishing emails from the EyeMed 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 EyeMed Email Account, and received inquiries from clients about the suspicious emails. EyeMed blocked the attacker's access to the EyeMed Email Account, and EyeMed's internal IT team began investigating the scope of the incident.

3.10.2. 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 EyeMed Email

Account during the time that the attacker was accessing the account. Investigators were unable to rule out that such exfiltration had occurred.

3.11. At the time of the Breach, while EyeMed had begun to roll-out Multi-Factor Authentication, EyeMed had not yet implemented Multi-Factor Authentication on the EyeMed Email Account.¹

3.12. At the time of the Breach, EyeMed, maintained an Office 365 E3 license. Due to the limitation with this license, EyeMed was unable to determine if email items were accessed; when email items were replied to or forwarded beyond 90 days; or identify when a user searched and what the user searched for.

3.13. At the time of the Breach, EyeMed set a minimum password length of eight characters and allowed for six failed login attempts before locking the account.

3.14. At the time of the Breach, EyeMed had an internal policy in place prohibiting the shared use of EyeMed email accounts from being utilized in the manner that the EyeMed Email Account was being utilized. Despite this internal policy, nine (9) EyeMed employees accessed the EyeMed Email Account by sharing and utilizing the same username and password amongst themselves.

3.15. Prior to the time of the Breach, EyeMed engaged third parties to conduct risk assessments. Those risk assessments did not evaluate EyeMed's email system.

3.16. On September 28, 2020, EyeMed began to notify Affected Consumers and regulators of the Breach.

3.17. Notifications to Affected Consumers continued on a rolling basis, through January 28, 2021.

¹ 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.

3.18. EyeMed offered Affected Consumers complimentary credit monitoring, fraud consultation, and identity theft restoration. For Affected Consumers who were minors, EyeMed offered Minor Social Security Number trace, fraud consultation, and identity theft restoration services.

3.19. EyeMed neither admits nor denies the Attorneys General's findings stated in Section 3 above.

4. ALLEGED VIOLATIONS OF LAW

4.1. The Attorneys General allege the following:

- 4.1.1. At all relevant times set forth in Section 3 above (the "Relevant Time Period"), incorporated herein by reference, EyeMed was and continues to be a Business Associate on behalf of Issuers, ASO Group Plans, and Resellers.
- 4.1.2. During the Relevant Time Period, EyeMed has offered services within the scope of the Consumer Protection Acts and the Personal Information Protection Acts.
- 4.1.3. During the Relevant Time Period, EyeMed maintained, stored, or managed computerized data including Personal Information within the scope of the Personal Information Protection Acts.
- 4.1.4. As a Business Associate, EyeMed was, and continues to be, required to comply with HIPAA standards governing the privacy and security of PHI, including, but not limited to the Security Rule, the Privacy Rule, and the Breach Notification Rule.
- 4.1.5. EyeMed violated the Consumer Protection Laws, the Personal Information Protection Acts, the Security Rule, and the Privacy Rule when it did not maintain reasonable security procedures designed to protect the confidentiality of PI and PHI of Affected Consumers.

4.1.6. Specifically, EyeMed failed to comply with the Security Rule and Privacy Rule by:

- i. Failing to ensure the confidentiality, integrity, and availability of the PHI of Affected Consumers contained in the EyeMed Email Account in violation of 45 C.F.R. § 164.306(a)(1);
- ii. Failing to conduct an accurate and thorough risk assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI in email, and to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A);
- iii. Failing to implement adequate procedures in the EyeMed Email Account for creating, changing, and safeguarding passwords in violation of 45 C.F.R. § 164.308(a)(5)(ii)(D);
- iv. Failing to implement security measures in the EyeMed Email Account sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B);
- v. Failing to implement technical policies and procedures for e-mail systems that maintain electronic protected health information to allow access only to those persons that have been granted access rights in violation of 45 C.F.R. § 164.312(a); and
- vi. Failing to implement procedures to verify that the person seeking access to PHI in the EyeMed Email Account is who they claim to be in violation of 45 C.F.R. § 164.312(d).

- 4.1.7. EyeMed's: (1) failure to ensure the proper security of the EyeMed Email Account; and (2) failure to properly retain and delete PHI and PI in the EyeMed Email Account, leading to the exposure of consumers' PHI and PI constitutes separate and additional unfair or deceptive practices, in violation of the Consumer Protection Acts.
- 4.1.8. EyeMed neither admits nor denies the Attorneys General's alleged violations of law stated in Section 4 above.

5. AGREED-UPON BUSINESS PRACTICES

A. Compliance with State and Federal Law

5.1. EyeMed shall comply with the Consumer Protection Acts, the Personal Information Protection Acts and HIPAA, including the Privacy Rule, Security Rule, and/or Breach Notification Rule, as applicable, in connection with a practice reasonably designed to secure PI or PHI against Security Incidents.

5.2. EyeMed shall not misrepresent the extent to which it maintains and protects the privacy, security, or confidentiality of PI or PHI collected from or about consumers.

B. Information Security Program

5.3. EyeMed shall continue to develop, implement, and maintain a written information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of PI, and PHI that EyeMed collects, stores, transmits, maintains, and/or destroys. The Information Security Program shall, at minimum, include the specific information requirements set forth in Paragraphs 5.4 through 5.23 of this Agreement, as modified by Section 8.8.

5.4. The Information Security Program shall comply with any applicable requirements under State or federal law, 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 PI or PHI that EyeMed collects, stores, transmits and/or maintains.

5.5. The Information Security Program shall be written and modified to allow access to PHI consistent with the Minimum Necessary Standard. EyeMed shall:

- i. Regularly monitor, log, and inspect network traffic, including log-in attempts, through the implementation of hardware, software, or procedural mechanisms that record and evaluate such activity;
- ii. Authorize and authenticate relevant device, user, and network activity within the EyeMed Network; and
- iii. Require appropriate authorization and authentication prior to any user's access to the EyeMed Network.

5.6. As part of its Information Security Program, EyeMed shall continue to implement and maintain a written incident response plan to prepare for and respond to Security Incidents. EyeMed shall review this response plan annually, then revise and update this response plan, as necessary, to adapt to any material changes that affect the security of PI and PHI. Such a plan shall, at a minimum, identify and describe the following phases: (i) Preparation; (ii) Detection and Analysis; (iii) Containment; (iv) Notification and Coordination with Law Enforcement; (v) Eradication; (vi) Recovery; (vii) Consumer and Regulator Notification and Remediation; and (viii) Post-Incident Analysis. If a Security Event does not trigger the Breach Notification Rule, the Consumer Protection Acts, or the Personal Information Protection Acts, EyeMed shall create a

report that includes a description of the Security Event and EyeMed's response to that Security Event ("Security Event Report").

5.7. EyeMed shall continue to employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program ("Chief Information Security Officer" or "CISO"). The CISO shall have the background and expertise in information security 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 PI and PHI that EyeMed collects, stores, transmits and/or maintains.

5.8. The Role of the CISO will include regular and direct reporting to EyeMed's Executive Staff, Senior Director of Information Security (HIPAA Security Officer), Senior Director of Privacy (HIPAA Privacy Officer), and other officers, as appropriate, concerning EyeMed's security posture and the risks faced by EyeMed. The CISO shall provide a tangible report to: (1) the Executive Staff on at least a semi-annual basis; and (2) the President, Senior Director of Information Security (HIPAA Security Officer), and Senior Director of Privacy (HIPAA Privacy Officer) on at least a quarterly basis. Such reports shall indicate any Security Events during the relevant time period.

5.9. All Security Events shall immediately be reported to the CISO, or their appointed representative in the event the CISO is unavailable, and in no event more than one calendar day from the identification of a Security Event. The CISO shall report to EyeMed's President, Senior Director of Information Security (HIPAA Security Officer), Senior Director of Privacy (HIPAA Privacy Officer), Executive Staff and officers, the Security Event within two business days of the CISO receiving notice of a Security Event.

5.10. The Information Security Program shall be memorialized in writing, maintained by the CISO, and represent EyeMed's most current Information Security Program appropriately and accurately. The CISO shall review the Information Security Program policies and standards at least annually. All substantive changes shall be tracked in a change log at the bottom of each document capturing the date on which the changes were made. If there are no changes made during a review process, the CISO shall acknowledge that in the change logs at the bottom of each document.

5.11. 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 management-level employees within sixty (60) days of the Effective Date of this Assurance or prior to their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

5.12. EyeMed shall continue to implement trainings required to comply with the Information Security Program to all employees.

C. Specific Information Security Requirements

5.13. **Data Collection & Retention:** EyeMed shall maintain reasonable policies and procedures governing its collection, use, and retention of PI and PHI. EyeMed shall limit its use, disclosure of, and requests for PHI in accordance with the Minimum Necessary Standard, to fulfill all applicable State and federal regulatory, and legal obligations.

5.14. **Cyber Security Operations Center ("C-SOC"):** EyeMed shall utilize a C-SOC or a reasonable equivalent technology. The C-SOC shall provide comprehensive monitoring of servers and other technologies, including those related to electronic mail, to identify possible

threats related to data, including PI and PHI. The C-SOC's analytic capabilities shall be deployed to detect, analyze, and escalate (as appropriate) Security Incidents.

5.15. **Logging & Monitoring:** EyeMed shall maintain reasonable policies and procedures designed to properly log and monitor, unless technologically unable to do so, the EyeMed Network and Covered Systems that collect, process, transmit, and/or store PI and PHI, in accordance with HIPAA. In furtherance of these policies and procedures, at minimum:

- i. EyeMed shall continue to employ tools such as a Security Information and Event Monitoring solution or a reasonably equivalent technology ("SIEM"), to log and monitor network traffic to detect and respond to Security Incidents.
- ii. EyeMed shall take reasonable steps to ensure the SIEM used pursuant to subsection (i) is properly configured, and regularly updated or maintained, and shall take reasonable steps to adequately log system activity and identify potential Security Incidents for review. Using the SIEM and/or other comparable security technology, EyeMed shall actively review and analyze in near real-time the logs of system activity and take appropriate follow-up actions with respect to Security Incidents. EyeMed shall create a formalized procedure to track Security Incidents and alerts, and EyeMed's response, on a regular basis.
- iii. 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.
- iv. Any logging and monitoring conducted pursuant to this paragraph shall be coordinated by the CISO and performed by appropriately trained and experienced personnel.

5.16. **Email Filtering and Phishing Solutions:** EyeMed shall maintain email protection and filtering solutions for all EyeMed's email accounts, including the filtering of unsolicited bulk emails, and protections from phishing attacks, and other email malware attacks.

5.17. **Access Controls:** EyeMed shall maintain appropriate controls to manage access to and use of all accounts that can access PI and PHI, including individual user accounts, administrator accounts, and vendor accounts. Controls shall include a reasonable means to regularly review access and access levels of users and remove network and remote access at the time of notification of termination for any employee whose employment has ended or any non-associate whose term has ended, in accordance with HIPAA.

5.18. **Authentication:** EyeMed shall maintain reasonable account management and authentication, including, but not limited to, individualized authentication credentials for every individual user account accessing EyeMed's Network. To the extent it is applicable, EyeMed shall forbid the use of shared individual user accounts without individualized authentication for each individual, shall require passwords be changed at least every ninety (90) days for individual user accounts, and shall require the use of Multifactor Authentication for all individual user accounts accessing EyeMed's internal network from an external network through VPN or an email-based service.

5.19. **Asset Inventory:** EyeMed shall maintain and regularly update a reasonable inventory of the assets that primarily comprise the EyeMed Network and appropriately identify and secure assets containing PI and PHI.

5.20. **Data Loss/Exfiltration Prevention:** EyeMed shall maintain a data loss prevention technology or a reasonably equivalent technology to detect and prevent unauthorized data exfiltration from the EyeMed Network.

5.21. **Encryption:** EyeMed shall maintain, regularly review, and revise policies and procedures to Encrypt PI and PHI at rest and in transit.

5.22. **Data Deletion:** EyeMed shall securely dispose of PI and PHI when there is no business or legal reason to retain it.

5.23. **Risk Assessments:** EyeMed shall maintain a risk assessment program to identify, address, and as appropriate, remediate risks affecting its Covered Systems.

5.24. **Information Security Program Assessment:** Within 120 days of the Effective Date and annually for three (3) years thereafter, for a total of four (4) assessments, EyeMed shall obtain an information security assessment of its policies from an independent third-party professional (“Third-Party Assessor”).

- i. The Third-Party Assessor must be an organization that employs at least one individual to perform the assessment that is: (a) qualified as a Certified Information System Security Professional (“CISSP”) or as a Certified Information Systems Auditor (“CISA”), or a similar qualification; and (b) has at least five (5) years of experience evaluating the effectiveness of computer systems and information system security.
- ii. The Third-Party Assessor shall prepare a report of findings (“Assessor Report”) that identifies all the areas where EyeMed stores PI and PHI, and includes: an assessment of all reasonably anticipated, internal, and external risks to the security, confidentiality, or availability of PI and PHI collected, processed, transmitted, stored, or disposed of by EyeMed; an assessment of EyeMed’s compliance with each of the requirements of this Assurance; an assessment of EyeMed’s response

to any Security Events which may have occurred since the Effective Date; and documentation of the basis of the Assessor Report.

- iii. The Assessor Report shall be maintained by the CISO and the HIPAA Privacy Officer.
- iv. Within thirty (30) days of completion of the Assessor Report, EyeMed shall notify the New Jersey Office of the Attorney General that the Assessor Report is available for inspection. EyeMed shall provide the Assessor Report to the New Jersey Office of the Attorney General upon written request.

5.25. On an annual basis for two (2) years following completion of the final Assessor Report required under 5.24, EyeMed shall provide the Attorneys General a Certification of Compliance with the terms of this AVC. Upon request, EyeMed shall make available to the New Jersey Office of the Attorney General the documents and materials that demonstrate its compliance with the terms of this AVC, including risk assessments conducted pursuant to 5.23 (“Compliance Materials”).

5.26. The New Jersey Office of the Attorney General shall, to the extent permitted by law, treat the Assessor Report and Compliance Materials as exempt from disclosure as applicable under the relevant public records laws of its state, provided that the New Jersey Office of the Attorney General may provide a copy of each Assessor Report and all Compliance Materials to New Jersey Attorney General’s office upon request. New Jersey Attorney General’s office shall, to the extent permitted by New Jersey law, treat such report and materials as exempt from disclosure as applicable under New Jersey public records law.

6. CONSUMER RELIEF

6.1. 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:

- i. 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.
- ii. 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
- iii. Social Security Number trace for minors.

7. SETTLEMENT PAYMENT

7.1. The Parties have agreed to a settlement of the Investigation in the amount of \$2,500,000 (“Settlement Payment”). This amount is to be divided and paid by EyeMed directly to the Attorneys General in an amount to be designated by and in the sole discretion of the States. The allocation of the Settlement Payment is not a finding or admission by EyeMed of liability.

7.2. EyeMed shall remit the Settlement Payment within fifteen (15) days after the Effective Date [except that where state law requires judicial or other approval of the Agreement, payment shall be made no later than fifteen (15) days after notice from the relevant Attorney General that such final approval for the Agreement has been secured].

7.3. Upon making the Settlement Payment, EyeMed shall immediately be fully divested of any interest in, or ownership of, the money paid. All interest in the Settlement Payment, and any subsequent interest or income derived therefrom, shall inure entirely to the benefit of the State pursuant to the terms herein.

7.4. The payment received by the New Jersey Attorney General may be used for purposes that may include, but are not limited to, attorneys’ fees, and other costs of investigation and litigation, or may be placed in, or applied to, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education or redress, litigation or local consumer aid fund or revolving fund, used to defray the costs of inquiry leading hereto, and/or for other uses permitted by New Jersey law at the sole discretion of the New Jersey Attorney General.

8. GENERAL PROVISIONS

8.1. This Agreement is entered into by the Parties as their own free and voluntary act and with full knowledge and understanding of the obligations and duties imposed by this Agreement.

8.2. This Agreement shall be governed by, and construed and enforced in accordance with, the laws of New Jersey.

8.3. The Parties have negotiated, jointly drafted, and fully reviewed the terms of this Agreement and the rule that uncertainty or ambiguity is to be construed against the drafter shall not apply to the construction or interpretation of this Agreement.

8.4. This Agreement contains the entire agreement among the Parties. Except as otherwise provided herein, this Agreement shall be modified only by a written instrument signed by or on behalf of the Parties.

8.5. Except as otherwise explicitly provided in this Agreement, nothing herein shall be construed to limit the authority of the Attorney General to protect the interests of New Jersey or the people of New Jersey.

8.6. If any portion of this Agreement is held invalid or unenforceable by operation of law, the remaining terms of this Agreement shall not be affected.

8.7. This Agreement shall be binding upon the Parties and their successors in interest. In no event shall assignment of any right, power, or authority under this Agreement void compliance with this Agreement.

8.8. This Agreement is entered into by the Parties for settlement purposes only. Neither the fact of nor any provision contained in this Agreement shall constitute or be construed as: (a) an approval, sanction, or authorization by the Attorneys General or any other governmental unit

of New Jersey of any act or practice of EyeMed; or (b) an admission by EyeMed that it violated the Consumer Protection Acts, the Personal Information Protection Acts, or HIPAA, including the Privacy Rule, Breach Notification Rule, and/or the Security Rule, or any other federal or State law, administrative rule or regulation, or an express or implied admission of any other matter of fact or law, or of any liability or wrongdoing. EyeMed's obligations under Paragraphs 5.5, 5.6, 5.13, 5.14, 5.15, 5.19, 5.20, and 5.23 shall expire at the conclusion of the five (5) year period after the Effective Date of this Agreement, unless they have expired at an earlier date pursuant to their specific terms.

8.9. EyeMed shall retain copies of any Security Event Report created pursuant to paragraph 5.6 for five (5) years from the date of the relevant Security Event.

8.10. This Agreement is not intended, and shall not be deemed, to constitute evidence or precedent of any kind in any action or proceeding except in an action or proceeding by one of the Parties to enforce, rescind, or otherwise implement any or all of the terms herein.

8.11. The Parties represent and warrant that their signatories to this Agreement have authority to act for and bind the respective Party.

8.12. Unless otherwise prohibited by law, any signatures by the Parties required for filing of this Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which shall constitute one and the same Agreement. Electronic signatures shall constitute acceptable, binding signatures for purposes of this Agreement.

9. PENALTIES FOR FAILURE TO COMPLY

9.1. The Attorneys General (or designated representative) shall have the authority to enforce the provisions of this Agreement or to seek sanctions for violations hereof or both.

10. COMPLIANCE WITH ALL LAWS

- 10.1. Except as provided in this Agreement, no provision herein shall be construed as:
- i. Relieving EyeMed of its obligations to comply with all State and federal laws, regulations, or rules, as now constituted or as may hereafter be amended; granting permission to engage in any acts or practices prohibited by any such laws, regulations, or rules; or requiring EyeMed to take an action that is prohibited by such laws, regulations, or rules; or
 - ii. Limiting or expanding any right the Attorneys General may otherwise have to obtain information, documents, or testimony from EyeMed pursuant to any State or federal law, regulation, or rule, as now constituted or as may hereafter be amended, or limiting or expanding any right EyeMed may otherwise have pursuant to any State or federal law, regulation, or rule, to oppose any process employed by the Attorneys General to obtain such information, documents, or testimony.

11. NOTICE

11.1. Except as otherwise provided herein, any notices or other documents required to be sent to the Attorneys General or EyeMed pursuant to this Agreement shall be sent by United States mail, Certified Mail Return Receipt Requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the documents and simultaneously by electronic mail. The notices and/or documents shall be sent to the following addresses:

For New Jersey:

Gina F. Pittore, Deputy Attorney General
Office of Attorney General
Department of Law and Public Safety
124 Halsey Street, 5th Floor

Newark, New Jersey 07101
Gina.Pittore@law.njoag.gov

For EyeMed:

Cathy Holley
General Counsel
EyeMed Vision Care LLC
4000 Luxottica Place
Mason OH 45040
cholley@eyemed.com

[Signature Pages to Follow]

IT IS ON THE 16th DAY OF May, 2023 SO ORDERED.

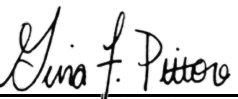
MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY

By: 
CARI FAIS, ACTING DIRECTOR
DIVISION OF CONSUMER AFFAIRS

THE PARTIES CONSENT TO THE FORM, CONTENT AND ENTRY OF THIS AGREEMENT ON THE DATES ADJACENT TO THEIR RESPECTIVE SIGNATURES.


FOR THE STATE:

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY

By: 
Gina F. Pittore
Deputy Attorney General
124 Halsey Street, 5th Floor
Newark, New Jersey 07101


Dated: May 15, 2023

FOR EYEMED VISION CARE LLC:


By: 
Matt MacDonald, President

Dated: May 15, 2023

FOR EYEMED VISION CARE LLC:

By: 
Sara Francescutto,
Chief Financial Officer

Dated: May 15, 2023

Reviewed As to Form by EyeMed Legal:


Appendix A

STATE	CONSUMER PROTECTION ACTS
Florida	Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Florida Statutes
New Jersey	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 <i>et seq.</i>
Oregon	Oregon Unlawful Trade Practices Act, ORS 646.605 <i>et seq.</i>
Pennsylvania	Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1 <i>et seq.</i>

Appendix B

STATE	PERSONAL INFORMATION PROTECTION ACTS & STATE BREACH NOTIFICATION ACTS
Florida	Florida Information Protection Act, Section 501.171, Florida Statutes
New Jersey	New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166
Oregon	Oregon Consumer Information Protection Act, ORS 646A.600 <i>et seq.</i>
Pennsylvania	Breach of Personal Information Notification Act, 73 P.S. §§ 2301 <i>et seq.</i>