Exhibit A1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

BARBARA WHITTOM, individually and on behalf of all others similarly situated, Plaintiff, v. EYEMED VISION CARE, LLC, Defendant.	Civil Action No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Barbara Whittom, individually, by and through her attorneys, brings this class action on behalf of herself and all similarly situated individuals against Defendant EyeMed Vision Care, LLC ("EyeMed" or "Defendant").

INTRODUCTION AND NATURE OF ACTION

1. Plaintiff Barbara Whittom brings this class action against EyeMed for its failure to secure its members' sensitive personal identifying information, including medical information ("PII").

2. EyeMed is a vision benefits company with a network of independent eye doctors, as well as national and regional retail eyewear setting providers, that includes LensCrafters, Pearle Vision, and Target Optical.

3. On July 1, 2020 EyeMed discovered that an unauthorized individual had gained access to an EyeMed email mailbox containing certain PII of current and former EyeMed members (the "Data Breach"), including full names, addresses, dates of birth,

phone numbers, email addresses, vision insurance account/identification numbers, health insurance account/identification numbers, Medicaid and Medicare numbers, driver's license or other government identification numbers, birth or marriage certificates, partial and full Social Security numbers, financial information, medical diagnoses and conditions, treatment information, and passport numbers.

4. Due to EyeMed's inadequate data security, Plaintiff and Class members have suffered irreparable harm and are subject to an increased risk of identity theft. Plaintiff's and Class members' PII has been compromised and they must now undertake additional security measures to minimize the risk of identity theft.

JURISDICTION AND VENUE

5. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

6. This Court has jurisdiction over EyeMed because EyeMed maintains its principal place of business in Ohio, regularly conducts business in Ohio and has sufficient minimum contacts in Ohio. EyeMed intentionally avails itself of this jurisdiction by marketing and selling services from Ohio to millions of consumers nationwide, including in Ohio.

7. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the

events, acts, and omissions giving rise to Plaintiff's and the Class members' claims occurred in this District.

PARTIES

8. Plaintiff Barbara Whittom is a resident of El Sobrante, California, and had her PII accessed, viewed and/or stolen as a result of the EyeMed Data Breach.

9. Defendant EyeMed is a vision benefits company with its principal place of business in Mason, Ohio. EyeMed's network includes independent eye doctors and national and regional retail eyewear setting providers including LensCrafters, Pearle Vision, and Target Optical. EyeMed's immediate corporate parent is Luxottica of North America, Inc.

FACTUAL BACKGROUND

10. EyeMed is the second largest vision benefits company in the United States, serving approximately 52 million members in large, medium, and small-sized companies, as well as government entities. EyeMed members are enrolled through employer-sponsored benefits sold directly by EyeMed or offered in partnership with healthcare organizations in the United States. EyeMed offers a network of eyecare providers in the United States, including a range of independent practitioners and retail locations that include Luxottica optical retail locations.

11. In the ordinary course of receiving health care services from EyeMed, Plaintiff and the Class members had to provide Defendant with sensitive PII, including, *inter alia*, names, addresses, dates of birth, phone numbers, email addresses, vision

insurance account and identification numbers, health insurance account and identification numbers, Medicaid or Medicare numbers, governmental identification numbers, social security numbers, financial information, information pertaining to medical diagnoses and conditions, and treatment information.

12. In its Notice of Privacy Practices, EyeMed asserts that it is "committed to protecting [members'] privacy," and promises, among other things, to: "Maintain the privacy and safeguard the security of your health information;" and "Notify [members], along with all other affected individuals, of a breach of unsecured health information."[1]

13. Additionally, EyeMed also promises that if it discovers that its members' health information has been breached, it "must notify you of the breach without unreasonable delay *and in no event later than 60 days following our discovery of the breach.*[2]

14. However, as described throughout this Complaint, EyeMed fell far short of its promise to maintain its members' privacy and failed to provide notice of the Data Breach within 60 days.

A. The Data Breach

15. On July 1, 2020, EyeMed discovered that one of its EyeMed email mailboxes had been accessed by an unauthorized individual. That email mailbox contained a trove of current and former members' PII, including:

- Full names

[1] https://eyemed.com/en-us/hipaa-notice-of-privacy-practices
[2] *Id.* (Emphasis added.)

- Addresses
- Dates of birth
- Phone numbers
- Email addresses
- Vision account and identification numbers
- Health insurance and identification numbers
- Medicaid and Medicare numbers
- Governmental identification numbers, including passports and driver's licenses
- Birth and marriage certificates
- Full and partial Social Security numbers
- Financial information
- Medical diagnoses and conditions
- Treatment information

16. On or about November 29, 2020, Plaintiff Whittom received a letter titled "Notice of Data Breach" from EyeMed, dated November 27, 2020. The letter stated that Plaintiff's PII, including those mentioned above, may have been compromised.

17. The information exposed by EyeMed is a virtual goldmine for phishers, hackers, identity thieves, and cybercriminals. This exposure is tremendously problematic.

18. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

19. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

20. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

21. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

22. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Here, EyeMed did not rapidly report to Plaintiff and Class members that their PII had been stolen. Instead, it took EyeMed over two months to notify them, despite its promise to provide notice of data breaches no longer than 60 days after discovery.

23. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

24. Data breaches facilitate identity theft as hackers obtain consumers' PII and then use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

25. For example, The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[3] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[4]

B. EyeMed Failed to Comply with Federal Trade Commission Requirements

26. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices.

[3] *See* Government Accountability Office, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007), available at http://www.gao.gov/assets/270/262899.pdf (last visited Jan. 15, 2021).
[4] *Id.*

According to the FTC, the need for data security should be factored into all business decision-making.[5]

27. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established guidelines for fundamental data security principles and practices for business. Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[6]

28. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[7]

29. Highlighting the importance of protecting against data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and

---

[5] *See* Federal Trade Commission, *Start with Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 15, 2021).
[6] *Id.*
[7] Federal Trade Commission, *Start with Security, supra* note 5.

reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

30. By allowing an unknown third party to access an EyeMed e-mail account with current and former members' sensitive PII, EyeMed failed to employ reasonable and appropriate measures to protect against unauthorized access to current and former member data. EyeMed's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

C. The Data Breach Was Foreseeable and Avoidable by EyeMed

31. EyeMed could have prevented the data breach from occurring. EyeMed failed to take adequate and reasonable measures to ensure its computer/server systems, including its email accounts, were protected against unauthorized access and failed to take actions that could have stopped the breach before it occurred.

32. EyeMed failed to disclose to Plaintiff and the Class members that their computer/server systems and data security practices were inadequate to reasonably safeguard Plaintiff's and Class members' PII and failed to immediately notify Plaintiff and the Class members of the data theft.

33. As a direct result of EyeMed's conduct, Plaintiff and the Class members were injured.

34. EyeMed was at all times fully aware of its obligations under the law and various standards and regulations to protect data entrusted to it by its members.

35. Despite EyeMed's awareness of its data protection obligations, EyeMed's treatment of the PII entrusted to it by its members fell short of satisfying its legal duties and obligations. EyeMed failed to ensure that access to its computer/server systems, including its email accounts, were reasonably safeguarded.

D. Plaintiff and Class Members Have Suffered Ascertainable Losses, Economic Damages, and Other Actual Injury and Harm

36. As a direct and proximate result of EyeMed's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and other Class members' PII, Plaintiff and the other Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the untimely notification of the Data Breach, (ii) loss of their benefit of the bargain with EyeMed; (iii) the resulting increased risk of future ascertainable losses, economic damages and other actual injury and harm, and (iv) the opportunity cost and value of lost time they must spend to monitor their personal, financial and payment card accounts—for which they are entitled to compensation.

CLASS DEFINITIONS AND ALLEGATIONS

37. Plaintiff brings this lawsuit as a class action on behalf of herself and all others similarly situated as members of the proposed classes pursuant to Federal Rules of Civil Procedure 23(a) and 23(b)(3):

A. The Nationwide Class

38. Plaintiff seeks to represent a class composed of United States residents (the "Nationwide Class"), defined as follows:

> All current and former members of EyeMed who reside in the United States and whose PII was maintained on EyeMed's email account that was compromised in the Data Breach.

B. The California Subclass:

39. Plaintiff seeks to represent a class composed of California residents (the "California Subclass"), defined as follows:

> All current and former members of EyeMed who reside in the State of California and whose PII was maintained on EyeMed's email account that was compromised in the Data Breach.

40. Collectively, the Nationwide Class and California Subclass will be referred to as "the Class" except where necessary to distinguish them.

41. Excluded from the proposed Class is Defendant EyeMed, including any entity in which Defendant has a controlling interest, is a subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant.

42. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

43. **Numerosity**: Although the exact number of Class members is uncertain and can only be ascertained through appropriate discovery, upon information and belief over 2,000,000 class members' information was affected, and, as such, joinder is impracticable. The disposition of the claims of these Class members in a single action

will provide substantial benefits to all parties and to the Court. The Class members may be identified from objective means, such as information and records in Defendant's possession, custody, or control.

44. **Commonality and Predominance**. Common questions of law and fact exist as to the proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's data security measures to protect Plaintiff's and the Class member's PII were reasonable in light of FTC data security recommendations, and best practices recommended by data security experts;

c. Whether Defendant's failure to implement adequate data security measures resulted in or was the proximate cause of the Data Breach;

d. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the loss of PII of Plaintiff and the Class members;

e. Whether Defendant owed a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, and safeguarding their PII;

f. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;

g. Whether Plaintiff and the Class members are at an increased risk for identify theft because of the Data Breach;

h. Whether Defendant's conduct violated Cal. Bus. & Prof. Code § 17200, *et seq*.

i. Whether Defendant violated section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiff's and Class members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure, as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information;

j. Whether Defendant violated the Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.*;

k. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

l. Whether Plaintiff and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

45. **Typicality**: Plaintiff's claims are typical of the claims of the Class. All Class members were subject to the Data Breach and had their PII accessed by unauthorized third parties.

46. **Adequacy of Representation**: Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

47. **Superiority**: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to

be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT ONE

Negligence
(On Behalf of Plaintiff and all Classes)

48. Plaintiff incorporates the allegations contained in paragraphs 1 through 47 as though fully set forth.

49. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security policies and systems to ensure that Plaintiff's and the Class members' PII was adequately secured and protected.

50. Defendant owed a duty of care to Plaintiff and members of the Class to provide security consistent with industry standards and to ensure that its systems and networks adequately protected the PII of its current and former members.

51. Defendant owed a duty of care to Plaintiff and members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of its current and former members and the critical importance of adequately securing such information.

52. Plaintiff and the members of the Class entrusted Defendant with their PII with the understanding that Defendant would safeguard their information and that Defendant was in a position to protect against the harm suffered by Plaintiff and members of the Class as a result of the Data Breach.

53. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members, including failing to implement the systems, policies, and procedures necessary to prevent the Data Breach.

54. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about—or should have been aware of—numerous, well-publicized data breaches affecting businesses in the United States.

55. Defendant breached its duties to Plaintiff and the Class members by failing to provide adequate computer policies, systems, and data security to safeguard the PII of Plaintiff and the Class members.

56. Because Defendant knew that a breach of its systems would damage its current and former members, including Plaintiff and the Class members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

57. Plaintiff and the Class members reasonably believed that Defendant would take adequate security precautions to protect their PII.

58. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class members' PII.

59. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class members' PII from being accessed, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class members.

60. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third party to access one or more of EyeMed's email accounts containing Plaintiff's and Class members' PII, Defendant violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures and failing to protect current and former EyeMed members' PII.

61. Plaintiff and the Class members are among the class of persons Section 5 of the FTC Act was designed to protect, and the injuries suffered by Plaintiff and the Class members is the type of injury Section 5 of the FTC Act was intended to prevent. As a result, Defendant is negligent per se.

62. Neither Plaintiff nor the other Class members contributed to the Data Breach as described in this Complaint.

63. As a direct and proximate cause of Defendant's conduct, Plaintiff and the Class members have suffered and/or will suffer injury and damages, including: (i) the loss of the benefit of their bargain with Defendant; (ii) the loss of the opportunity to determine for themselves how their PII is used; (iii) the publication and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (viii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of current and former members in its continued possession; and, (ix) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the consequences of compromised PII for the rest of their lives.

COUNT TWO

Breach of Express Contract
(On Behalf of Plaintiff and all Classes)

64. Plaintiff incorporates the allegations set forth in paragraphs 1 through 47 as though fully set forth.

65. Defendant knew or should have known that the PII Plaintiff and Class members provided to Defendant was highly confidential and sensitive.

66. Defendant's Privacy Policy is an agreement between Defendant and members who provide PII to Defendant, which includes Plaintiff and Class members.

67. At all relevant times, Defendant expressly represented in its Notice of Privacy Practices that it was required by law to, *inter alia*, "Maintain the privacy and safeguard the security of your health information;" and "Notify you, along with all other affected individuals, of a breach of unsecured health information." Defendant also expressly promised in its Notice of Privacy Practices that if it discovered that its members' health information had been breached, "we must notify you of the breach without unreasonable delay and in no event later than 60 days following our discovery of the breach."

68. Defendant's current and former members, including Plaintiff and Class members, gave Defendant PII for healthcare benefits. Plaintiff and Class members therefore demonstrated their willingness and intent to enter into a bargain with Defendant and assent to the terms of the Privacy Policy by giving their PII to Defendant.

69. Plaintiff and Class members therefore entered into a contract with Defendant when providing PII to Defendant subject to the terms of the Privacy Policy.

70. Plaintiff and Class members have upheld their obligations under the agreement. Defendant, on the other hand, breached its obligations by failing to implement reasonable security measures, which led to unauthorized disclosure of PII to third parties.

71. Defendant further breached its obligations by failing to inform Plaintiff and Class members of the Data Breach no later than 60 days following its discovery of the Data Breach.

72. As a direct and proximate result of Defendant's breach of this agreement, Plaintiff and Class members did not receive the benefit of their bargain with Defendant and were injured as described in detail herein.

COUNT THREE

Breach of Implied Contract
(On Behalf of Plaintiff and all Classes)

73. Plaintiff incorporates the allegations contained in paragraphs 1 through 47 as though fully set forth herein.

74. Plaintiff and the Class members entered into an implied contract with Defendant by providing their PII to Defendant when using services provided by Defendant. Implied in these exchanges was a promise by Defendant to implement reasonable procedures and practices to protect the PII of Plaintiff and the Class members and to timely notify them in the event their PII was compromised.

75. Plaintiff and the Class members reasonably expected that Defendant had implemented adequate security measures to protect their PII and would allocate a portion of the money paid by Plaintiff and the Class members under the implied contracts to fund those security measures.

76. Neither Plaintiff nor the Class members would have provided their PII to Defendant or paid the same fees to Defendant or its subsidiaries for services without this implied contract between them and Defendant. Defendant needed to adequately safeguard Plaintiff's and Class members' PII and provide timely notice of a data breach to realize the intent of the parties.

77. Plaintiff and Class members performed their obligations under the implied contracts with Defendant. Conversely, Defendant breached its obligations under the implied contracts by (i) failing to implement reasonable security procedures and practices to protect Plaintiff's and the Class members' PII; (ii) enabling unauthorized access of PII by third parties due to the inadequate security measures; and (iii) failing to provide timely notice of the Data Breach.

78. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and the Class members did not get the benefit of their bargain with Defendant and were injured as described in detail above.

COUNT FOUR

Violations of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, et seq.
(On Behalf of Plaintiff and the California Subclass)

79. Plaintiff incorporates the allegations contained in paragraphs 1 through 47 as though fully set forth herein.

80. Defendant's business practices as complained of herein violate California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. ("UCL").

81. Defendant's practices constitute "unlawful" business practices in violation of the UCL because, among other things, they violate statutory law and the common law, including, without limitation, the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, et seq., and Section 5 of the FTC Act.

82. Defendant's actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiff and the California Subclass members outweighs the utility of Defendant's conduct. This conduct includes Defendant's failure to adequately ensure the privacy, confidentiality, and security of members' data entrusted to it and Defendant's failure to have adequate data security measures in place.

83. As a result of Defendant's wrongful business practices, Plaintiff and members of the California Subclass have suffered injury in fact and lost money or property as alleged herein.

84. Defendant's wrongful business practices present an ongoing and continuing threat to Plaintiff and the California Subclass members.

85. Accordingly, Plaintiff and the California Subclass members have and will incur economic damages related to the Data breach including loss of the benefit of their bargain with Defendant; time and money spent remedying the Data Breach; experiencing lack of access to funds while banks and financial institutions issue new cards; and the costs of credit monitoring, purchasing credit reports, and purchasing "freezes" to prevent opening of unauthorized accounts.

COUNT FIVE

Violations of California's Consumer Privacy Act Cal. Civ. Code § 1798.150, et seq. (On Behalf of Plaintiff and the California Subclass)

86. Plaintiff incorporates the allegations contained in paragraphs 1 through 47 as though fully set forth herein.

87. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140. As a result, Defendant has a duty to implement and maintain reasonable security procedures and practices to protect this personal information. As alleged herein, Defendant failed to do so.

88. Defendant EyeMed is a corporation organized for the profit or financial benefit of its owners, and, on information and belief, has annual gross revenues exceeding $25 million and collects PII as defined in Cal. Civ. Code § 1798.140. In addition, Defendant EyeMed annually buys, receives, sells, or shares for commercial

purposes the PII of more than 50,000 consumers.

89. Upon information and belief, Defendant violated § 1798.150 of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff and California Subclass members' nonencrypted and nonredacted PII from unauthorized access, and exfiltration, theft, or disclosure. These failures were the result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

90. As a direct and proximate result of Defendant's conduct, Plaintiff and the California Subclass members' PII, including names, payment card numbers, and Social Security numbers, was subjected to unauthorized access, exfiltration, theft, or disclosure. On information and belief, Plaintiff alleges that this PII was not encrypted or redacted in the format accessed during the Data Breach.

91. Plaintiff and the California Subclass members seek injunctive or other equitable relief to ensure Defendant hereafter adequately safeguards customers' PII by implementing reasonable enhanced security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including that of Plaintiff and the California Subclass. These individuals have an interest in ensuring that their PII is reasonably protected.

92. On December 22, 2020 Plaintiff's Counsel mailed a notice letter to Defendant's registered service agent as required under Cal. Civ. Code § 1798.150(b). Assuming Defendant cannot cure the Data Breach within 30 days, and Plaintiff believes any such cure is not possible under these facts and circumstances, Plaintiff will amend

this complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

COUNT SIX

Violations of California's Confidentiality of Medical Information Act Cal. Civ. Code § 56, et seq. (On Behalf of Plaintiff and the California Subclass)

93. Plaintiff incorporates the allegations contained in paragraphs 1 through 47 as though fully set forth.

94. Defendant is a "health care service plan," within the meaning of Civil Code § 56.05(g), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), of "enrollees" and/or "subscribers" of Defendant, within the meaning of Civil Code §§ 56.05(f), 56.05(o).

95. Plaintiff and California Subclass members are "enrollees" and/or "subscribers" of Defendant within the meaning of Civil Code §§ 56.05(f), 56.05(o), and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiff and the California Subclass members fear that disclosure of their medical information could subject them to harassment or abuse. Furthermore, Plaintiff and California Subclass members, as enrollees and/or subscribers of Defendant, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network, and were enrollees and/or subscribers on or before July 1, 2020.

96. Defendant negligently created, maintained, preserved, stored, and then exposed Plaintiff's and California Subclass members' individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), including Plaintiff's and California Subclass members' vision insurance account and identification numbers, health insurance account and identification numbers, Medicaid and Medicare numbers, medical diagnoses and conditions, and treatment information.

97. Defendant negligently created, maintained, preserved, stored, and released Plaintiff's and Class members' medical information in violation of Civil Code § 56.101(a).

98. Defendant violated Civil Code § 56.101(a) of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the California Subclass.

99. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and the California Subclass members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. On information and belief, Plaintiff's and California Subclass members' medical information was viewed by an unauthorized individual(s) as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

100. Plaintiff's and California Subclass members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

101. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. On information and belief, Plaintiff's and California Subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

102. As a result of Defendant's above-described conduct, Plaintiff and the California Subclass have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.101 and 56.36.

103. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the California Subclass members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

104. Plaintiff, individually and for each member of the Class, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), and damages provided by the common law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the proposed Class as requested herein;
b. Appointing Plaintiff as Class Representative and undersigned counsel as Class Counsel;
c. Finding that Defendant engaged in the unlawful conduct as alleged herein;
d. Enjoining Defendant's conduct and requiring Defendant to implement proper data security policies and practices, including:
    i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein,
    ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws,
    iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff and the Class members unless Defendant can provide to the Court reasonable

justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class members,

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and the Class members' PII,

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors,

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring,

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures,

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems,

ix. requiring Defendant to conduct regular database scanning and securing checks,

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and the Class members,

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII,

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,

xiv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII to third

parties, as well as the steps affected individuals must take to protect themselves,

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers,

xvi. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected,

xvii. requiring Defendant to disclose any future data breaches in a timely and accurate manner,

xviii. requiring Defendant to implement multi-factor authentication requirements, and

xix. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices.

e. Awarding Plaintiff and Class members damages;

f. Awarding Plaintiff and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMAND

Plaintiff, on behalf of herself and the proposed Class, hereby demands a trial by jury as to all matters so triable.

Respectfully submitted,

Dated: January 22, 2021

/s/ Andrew P. Schabo

ANDREW P. SCHABO (OH # 0082988)
MANCINI SMITH LAW
32 W. Hoster Street, Suite 200
Columbus, OH 43215
Telephone: (614) 300-5001
Facsimile: (614) 223-2102
andrews@mancinilaw.com

David S. Casey, Jr., *Pro Hac Vice forthcoming*
Gayle M. Blatt, *Pro Hac Vice forthcoming*
Jeremy Robinson, *Pro Hac Vice forthcoming*
P. Camille Guerra, *Pro Hac Vice forthcoming*
Catherine M. McBain, *Pro Hac Vice forthcoming*
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
dcasey@cglaw.com
gmb@cglaw.com
jrobinson@cglaw.com
camille@cglaw.com
kmcbain@cglaw.com

Attorneys for Plaintiff and the Class