Exhibit A2

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

CHANDRA TATE, BARBARA WHITTOM and ALEXUS WYNN, on behalf of themselves and all others similarly situated, Plaintiffs, v. **EYEMED VISION CARE, LLC,** Defendant.	Case No. 1:21-cv-00036-DRC Judge Douglas R. Cole **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Chandra Tate, Barbara Whittom, and Alexus Wynn (collectively "Plaintiffs"), by and through their attorneys, upon personal knowledge as to themselves and their own acts and experiences, and upon information and belief as to all other matters, including their counsel's investigation, allege as follows. Plaintiffs believe additional evidentiary support exists for their allegations, given an opportunity for discovery.

NATURE OF THE ACTION

1. Plaintiffs bring this Consolidated Class Action Complaint ("Complaint") against Defendant EyeMed Vision Care, LLC ("Defendant" or "EyeMed"), individually and on behalf of all others similarly situated based on Defendant's failure to properly safeguard its customers' personally identifiable information ("PII"), including current and former customers' full names, residential addresses, dates of birth, phone numbers, email addresses, vision insurance account identification numbers, health insurance account identification numbers, Medicaid and Medicare numbers, Social Security numbers, birth or marriage certificates, and driver's license, passport or

other government identification numbers and information. Defendant also failed to properly safeguard its customers' protected health information ("PHI") exposed in the breach, including medical diagnoses and medical treatment information.

2. EyeMed is one of the largest and fastest growing vision benefits companies in the United States. It has over 60 million funded benefit members through a nationwide network of providers that includes optometrists, ophthalmologists, opticians, and retailers. EyeMed offers several different plans, all of which provide various levels of discounts on exams and vision products such as eyeglass frames and lenses, contact lenses, and other eye care services. The company serves a customer base that includes large corporations, government entities, and health insurers, including but not limited to Aetna, Blue Cross Blue Shield of Tennessee, and Nippon Life Benefits.

3. On June 24, 2020, as a result of EyeMed's lax security and monitoring protocols, criminals gained unauthorized access to an EyeMed email inbox (the "Data Breach"). For seven days, these criminals maintained unfettered access to the breached email account. During this time, the email account was used to send phishing emails to EyeMed's customers. The Data Breach also allowed the criminals to obtain the sensitive PII and PHI of EyeMed's customers stored in the account.

4. It was not until July 1, 2020 that EyeMed discovered the Data Breach and took steps to block unauthorized access to the account. By that time, the PII and PHI of its customers had already fallen into the hands of the ill-intentioned criminals that accessed the account.

5. Defying all bounds of reasonableness, despite learning of the Data Breach on or about July 1, 2020, EyeMed did not begin notifying customers affected by the breach until late November and December 2020. And it did not prioritize the victims of the breach; instead, months

before it started notifying customers, EyeMed notified its industry partners such as Aetna. There is simply no excuse for taking so long to notify customers, and for de-prioritizing the actual victims of its lax security and safeguards.

6. EyeMed did not adequately safeguard Plaintiffs' data, and now they and apparently millions of other patients are the victims of a significant data breach that will negatively affect them for years.

7. EyeMed is responsible for allowing this Data Breach through its failure to implement and maintain reasonable safeguards and failure to comply with industry-standard data security practices as well as federal and state laws and regulations governing data security, including security of PHI.

8. Despite its role in managing so much sensitive and personal PII and PHI, during the duration of the data breach, EyeMed failed to recognize and detect unauthorized third parties accessing its email system, and failed to recognize the substantial amounts of data that had been compromised. This was, in part, because of, but also part and parcel with, EyeMed's failure to take the appropriate steps to investigate the numerous red flags, each of which individually should have told EyeMed that its systems were not secure.

9. During the duration of the Data Breach, EyeMed failed to, among other things, detect that ill-intentioned criminals had accessed its computer data and storage systems, notice the massive amounts of data that were compromised, take any steps to investigate the red flags that should have warned EyeMed that its systems were not secure. Had EyeMed properly monitored its information technology infrastructure, it would have discovered the invasion sooner.

10. EyeMed had numerous statutory, regulatory, contractual, and common law obligations, including those based on its affirmative representations to Plaintiffs and Class

members, to keep their PII, including PHI, confidential, safe, secure, and protected from unauthorized disclosure or access, specifically including the Health Insurance Portability and Accountability Act of 1996 ("HIPPA"). Plaintiffs and those similarly situated rely upon EyeMed to maintain the security and privacy of the PII and PHI entrusted to it; when providing their PII and or PHI, they reasonably expected and understood that EyeMed would comply with its obligations to keep the information secure and safe from unauthorized access.

11. In this day and age of regular and consistent data security attacks and data breaches, in particular in the healthcare industry and retail services, EyeMed's Data Breach is particularly egregious.

12. By obtaining, collecting, using, and deriving benefit from Plaintiffs' and Class members' PII an PHI, EyeMed assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and class members' PII and PHI from disclosure.

13. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their PII and PHI.

14. Plaintiffs and Class members relied on EyeMed to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

15. As a result of EyeMed's failures to protect the PII and PHI of Plaintiffs and Class members, their PII and PHI were accessed by malicious cyber criminals. Therefore, Plaintiffs and the Class members are at a significant present and future risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come. Just as their PII and PHI was stolen because of its inherent value in the black market, now the inherent value of Plaintiffs and the Class members' PII and PHI in the legitimate market is significantly and materially

decreased. To make matters worse, the injuries described were exacerbated by EyeMed's failure to timely inform and notify Plaintiffs and the Class members of the data breach and their injuries. Furthermore, by failing to provide adequate notice, EyeMed intentionally prevented Plaintiffs and prospective Class members from protecting themselves from the potential damages arising out of the data breach.

16. On information and belief, as a result of this massive data breach, over a million of EyeMed's customers have suffered exposure of PII and PHI entrusted to EyeMed.

17. In addition, based on Defendant's actions, Plaintiffs and the proposed Class have received services that were and are inferior to those for which they have contracted, and have not been provided the protection and security Defendant promised when Plaintiffs and the proposed class entrusted Defendant with their PII and PHI.

18. Plaintiffs and members of the proposed Class have suffered actual and imminent injuries as a direct result of the Data Breach. The injuries suffered by Plaintiffs and the proposed Class as a direct result of the Data Breach include: (a) theft of their personal data; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the consequences of the Data Breach and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach; (d) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (e) damages to and diminution in value of their personal data entrusted to EyeMed and with the mutual understanding that EyeMed would safeguard Plaintiffs' and Class members' personal data against theft and not allow access and misuse of their personal data by others; (f) the reasonable value of the PII entrusted to EyeMed;

and (g) the continued risk to their personal data, which remains in the possession of EyeMed and which is subject to further breaches so long as EyeMed fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' personal data in its possession.

19. Plaintiffs seek to remedy these harms, and prevent their future occurrence, on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach.

20. Accordingly, Plaintiffs, on behalf of themselves and other members of the Class, assert claims for breach of implied contract, negligence, unjust enrichment, and Plaintiff Whittom and the California Subclass also assert claims for violations of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL"), of California's Confidentiality of Medical Information Act, Cal. Civ. Code §1798.100, *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.* and seek injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

21. Plaintiff Chandra Tate[1] is a natural person and a resident of South Carolina. Plaintiff Tate is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Tate's PII and PHI and has a legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure. Plaintiff Tate would not have entrusted her PII and PHI to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff Tate's PII and PHI was compromised and disclosed as a result of the Data Breach.

22. Plaintiff Barbara Whittom is a natural person and a resident of California. Plaintiff

[1] Plaintiff Tate's name was previously Chandra Price. However, she married in February 2020 and assumed the surname of Tate.

Whittom is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Whittom's PII and PHI and has a legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure. Plaintiff Whittom would not have entrusted her PII and PHI to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff Whittom's PII and PHI was compromised and disclosed as a result of the Data Breach.

23. Plaintiff Alexus Wynn is a natural person and a resident of South Carolina. Plaintiff Wynn is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Wynn's PII and PHI and has a legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure. Plaintiff Wynn would not have entrusted her PII and PHI to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff Wynn's PII and PHI was compromised and disclosed as a result of the Data Breach.

24. EyeMed is a Delaware limited liability company with its principal place of business in Mason, Ohio. It is a wholly owned subsidiary of Luxottica of America, Inc., which is similarly headquartered in Mason, Ohio.

JURISDICTION & VENUE

25. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Plaintiffs (and many members of the Class) and Defendant are citizens of different states.

26. This Court has general personal jurisdiction over EyeMed because EyeMed's principal place of business is, and does regularly conduct business, in Mason, Ohio.

27. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and EyeMed conducts substantial business in this District.

FACTUAL ALLEGATIONS

As a Vision Benefits Company, EyeMed Collects PII and PHI from its Members and Knew it was and Continues to be a Prime Target for Cyberattacks

28. EyeMed is one of the largest vision benefits companies in the United States, providing vision benefits to over 60 million members.[2] As of 2014, it was the second largest vision benefits companies in the United States.[3]

29. In the course of providing services to its members, EyeMed acquires, collects, and stores or processes a massive amount of PII and PHI on its members, including (1) contact information (including, but not limited to, name, email, and address); (2) financial information (including, but not limited to, name, health savings account, etc.); and (3) medical history. This information comes from the customers and from other individuals or organizations, such as referring physicians, other doctors, and/or insurance plans.

30. As a condition of providing vision benefit from EyeMed, EyeMed requires that its members entrust it with highly sensitive PII and PHI.

31. EyeMed requires its customers to provide contact information (such as name, email, and address), and financial information (such as Health Savings Account or other credit card account information). As part and parcel of providing and/or accepting insurance, customers must also provide their sensitive health information and other personal information (such as dates of birth and Social Security numbers, that EyeMed requests).

[2] https://eyemed.com/en-us/about-us (last visited April 20, 2021).
[3] https://en.wikipedia.org/wiki/Luxottica (last visited April 20, 2021).

32. As with all benefit or insurance companies, upon information and belief, use of EyeMed's services requires disclosure of PII and PHI to EyeMed by all of its over 60 million members.

33. Moreover, EyeMed provides that each of its affiliates are permitted to share customer PII and other information across brands.

34. EyeMed is fully aware of how sensitive the PII and PHI it stores and maintains is. It is also aware of how much PII and PHI it collects, uses, and maintains from each Plaintiff or Class member. EyeMed offers services related to healthcare treatment and the provision of insurance.

35. The seriousness with which EyeMed should have taken its data security is shown by the number of data breaches perpetrated in the healthcare and retail industries in the last few years.

36. Over 41 million patient records were breached in 2019, with a single hacking incident affecting close to 21 million records.[4] Healthcare breaches in 2019 almost tripled those the healthcare industry experienced in 2018, when 15 million patient records were affected by data breach incidents, according to a report from Protenus and DataBreaches.net.[5]

37. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents disclosed to the U.S. Department of Health and Human Services or the media during 2019, finding that there has been an alarming increase in the number of data breaches of patient privacy since

[4] Heather Landi, *Number of patient records breached nearly triples in 2019*, Fierce Heathcare (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=Over%2041%20million%20patient%20records,close%20to%2021%20million%20records. (last visited April 30, 2021).

[5] *Id.*

2016, when there were 450 security incidents involving patient data. [6] In 2019 that number jumped to 572 incidents, which is likely an underestimate, as two of the incidents for which there were no data affected 500 dental practices and clinics and could affect significant volumes of patient records. There continues to be at least one health data breach per day.[7]

38. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiffs' and the Class members' PII and PHI, EyeMed assumed certain legal and equitable duties and knew or should have known that it was responsible for the diligent protection of the PII and PHI it collected and stored.

EyeMed knew that it was and continues to be a prime target for cyberattacks.

39. EyeMed knew that it was an ideal target for hackers and those with nefarious purposes related to consumers data. It processed and saved multiple types and many levels of PII and PHI through its computer data and storage systems.

40. Realizing that its data is a target of hackers, EyeMed's Privacy Policy[8] states:

> The security of your personal information 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.

41. Yet, EyeMed did not follow generally accepted industry standards to protect its customers' sensitive PII and PHI.

42. EyeMed processed employer and payment information, in addition to all the information about vision, vision healthcare, and any other information that it might demand as a benefits provider, such as Social Security number, age, gender, and prior health history.

---

[6] *Id.*
[7] *Id.*
[8] https://eyemed.com/en-us/online-privacy-policy (last visited April 20, 2021).

43. Despite knowledge of the prevalence of healthcare and retail data breaches, EyeMed failed to prioritize its customers' data security by implementing reasonable data security measures to detect and prevent unauthorized access to the tens of millions of sensitive data points of its customers. As a highly successful insurance benefits company, EyeMed had the resources to invest in the necessary data security and protection measures. Yet, it did not.

44. EyeMed failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures that occurred in June 2020 about which its customers were not notified until November and December 2020.

45. Despite its awareness, EyeMed did not take the necessary and required minimal steps to secure Plaintiffs' and the Class members' PII and PHI. As a result, hackers breached and stole important PII and PHI from over one million EyeMed customers in late June 2020.

The Data Breach and EyeMed's Failure to Timely Notify Victims of the Data Breach

46. On July 1, 2020, EyeMed became aware that the Data Breach occurred. Specifically, a cybercriminal gained access to an email account and sent phishing emails to contacts from the account's address book on the same day. An investigation determined the hacked account contained information from EyeMed's current and former vision benefits' members. The data included member names, contact details, dates of birth, health insurance account and identification numbers, Medicaid or Medicare numbers, driver's licenses and other government identification numbers.

47. EyeMed did not notify the victims of the breach at that time or for months later. Rather, it first notified large corporations that it partners with or performed services for. For example, almost three months after it learned of the breach, on September 28, 2020, EyeMed informed the insurance company Aetna of the breach, which had exposed the PII and PHI of

approximately 484,157 Aetna customers alone.[9]

48. Inexplicably, it was not until almost six months after the breach (mid-December 2020) that EyeMed took the necessary step of informing individuals such as Plaintiffs and members of the Class via letter that it "discovered that an unauthorized individual gained access to an EyeMed email mailbox and sent phishing emails to email addresses contained in the mailbox's address book." For example, Plaintiff Tate received the following in a letter (attached as **Exhibit A**) received in mid-December 2020 and dated December 7, 2020:

> On July 1, 2020, EyeMed discovered that an unauthorized individual gained access to an EyeMed email mailbox and sent phishing emails to email addresses contained in the mailbox's address book….It was determined that the unauthorized individual first gained access to the mailbox on June 24, 2020, and that access terminated on July 1, 2020.
> …
> The mailbox contained information about individuals who formerly or currently receive vision benefits through EyeMed.
> …
> Following a detailed analysis and review of all potentially compromised emails and files, EyeMed identified the names of all individuals who were impacted, as well as the type of information included in those files. Personal information that may have been accessed could include the following types of information: full name, address, date of birth, phone number, email address, and vision insurance account/identification number.

49. EyeMed's letter to Plaintiffs and members of the Class was patently deficient because it failed to disclose the full range of information that may have been compromised in the breach. For example, EyeMed's website discloses information that was exposed in the breach but not mentioned in its letters to Plaintiffs and members of the Class, including: health insurance account/identification numbers, Medicaid or Medicare numbers, driver's license or other government identification numbers, birth or marriage certificates, Social Security numbers,

[9] https://www.healthcareitnews.com/news/nearly-500k-aetna-members-affected-eyemed-security-incident (last visited April 20, 2021).

financial information, medical diagnoses and conditions, treatment information, and/or passport numbers.[10]

50. EyeMed's disclosure letter also described what it was doing to remedy its flawed security protocols:

> EyeMed is committed to safeguarding your personal information and has taken immediate steps to enhance the protections that were already in place before this incident. In addition to the investigation, EyeMed made changes to how authorized individuals access the EyeMed network and required immediate complex password changes to all our employee accounts. EyeMed is also reinforcing and providing additional mandatory security awareness training.

51. EyeMed "encourage[d]" Plaintiffs and the Class members "to remain vigilant," and told them that if they see suspicious or unusual activity on their accounts, **not to tell EyeMed**, but to report it to someone else.

52. Despite knowing about the Data Breach since July 1, 2020, EyeMed did not issue notice to those affected within the timeframe required by law or its own Privacy Policy.

53. For example, in its HIPAA Notice of Privacy Practices, EyeMed states:

> If we discover that your health information has been breached (for example, disclosed to or acquired by an unauthorized person, stolen, lost, or otherwise used or disclosed in violation of applicable privacy law) and the privacy or security of the information has been compromised, we must notify you of the breach without unreasonable delay and in *no event later than 60 days following our discovery of the breach*.[11]

Plaintiff Tate's Experience

54. From 2016 through 2019, Plaintiff Tate and her family used EyeMed for their vision care benefits. This included submitting claims to EyeMed for the purchase of prescription lenses from Walmart and Sam's Club.

55. Plaintiff Tate entrusted her PII, PHI, and other confidential information such as

[10] *See* https://eyemed.com/en-us/notice (last visited April 20, 2021).
[11] https://eyemed.com/en-us/hipaa-notice-of-privacy-practices (last visited April 20, 2021) (emphasis added).

contact information, health insurance policy information, prescription information, medical conditions, and Social Security number to EyeMed with the reasonable expectation and understanding that EyeMed would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have used EyeMed's services had she known that EyeMed would not take reasonable steps to safeguard her sensitive PII and PHI.

56. In December 2020, more than five months after EyeMed learned of the Data Breach, Plaintiff Tate received a letter from EyeMed, dated December 7, 2020, notifying her that her PII and PHI had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Tate's PII and PHI, including her full name, address, date of birth, phone number, email address, and vision insurance account/identification number, was compromised as a result of the Data Breach. A copy of the letter is attached hereto as **Exhibit A**.

57. As a result of the Data Breach, Plaintiff Tate made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letter, including but not limited to continuing to maintain credit monitoring from LifeLock for approximately $53 per month, a charge that she was going to discontinue prior to the Data Breach to reduce her monthly expenses. In addition, Plaintiff Tate spent time researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Tate now spends approximately one hour daily reviewing her bank statements and credit card accounts for irregularities. This is valuable time Plaintiff Tate otherwise would have spent on other activities, including but not limited to work and/or recreation.

58. Plaintiff Tate suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII and PHI, a form of property that EyeMed obtained from Plaintiff Tate; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

59. Moreover, subsequent to the Data Breach, Plaintiff Tate also experienced actual identity theft and fraud, including notification that her private information was found on the dark web and a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages. Plaintiff Tate has received scam and phishing phone calls nearly every day since the Data Breach. For example, towards the end of November 2020, Plaintiff Tate received calls from scammers purporting to work for the Internal Revenue Service and Social Security Administration.

60. Plaintiff Tate has spent approximately 12 hours per month responding to incidents related to the Data Breach and activities trying to mitigate the impact of the Data Breach. This is time Plaintiff Tate otherwise would have spent on other activities, such as work and/or recreation.

61. As a result of the Data Breach, Plaintiff Tate has suffered emotional distress as a result of the release of her PII and PHI and her daughter Plaintiff Wynn's PII and PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of identity theft and fraud. Plaintiff Tate is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

62. As a result of the Data Breach, Plaintiff Tate anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

In addition, Plaintiff Tate will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Whittom's Experience

63. From 2012 through 2015 and again in 2019, Plaintiff Whittom used EyeMed for her vision care benefits. This included submitting claims to EyeMed for the purchase of prescription lenses from LensCrafters and Dr. Scott Lee.

64. Plaintiff Whittom entrusted her PII, PHI, and other confidential information such as contact information, health insurance policy information, prescription information, medical conditions, and Social Security number to EyeMed with the reasonable expectation and understanding that EyeMed would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have used EyeMed's services had she known that EyeMed would not take reasonable steps to safeguard her sensitive PII and PHI.

65. In November 2020, more than five months after EyeMed learned of the data breach, Plaintiff received a letter from EyeMed, dated November 27, 2020, notifying her that her PII and PHI had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Whittom's PII and PHI, including her full name, address, date of birth, full or partial Social Security number, Health Insurance/Member ID Number, and/or other personal or financial information, was compromised as a result of the Data Breach. A copy of the letter is attached hereto as **Exhibit B**.

66. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letter, including but not

limited to researching and enrolling in the credit monitoring and identity theft protection services offered by Defendant. In addition, Plaintiff Whittom spent time researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Whittom has spent approximately 30 hours since the Data Breach reviewing her bank statements and credit card accounts for irregularities. This is valuable time Plaintiff Whittom otherwise would have spent on other activities, including but not limited to work and/or recreation.

67. Plaintiff Whittom suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII and PHI, a form of property that EyeMed obtained from Plaintiff Whittom; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

68. Moreover, subsequent to the Data Breach, Plaintiff Whittom also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages. For example, Plaintiff Whittom has received scam and phishing phone calls from scammers purporting to work Social Security Administration and other calls threatening arrest daily. Plaintiff Whittom has also received scam emails from Amazon and Best Buy.

69. Plaintiff Whittom has spent at least 36 hours responding to incidents related to the Data Breach and activities trying to mitigate the impact of the Data Breach. This is time Plaintiff Whittom otherwise would have spent on other activities, such as work and/or recreation.

70. As a result of the Data Breach, Plaintiff Whittom has suffered emotional distress as a result of the release of her PII and PHI, which she believed would be protected from unauthorized

access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of identity theft and fraud. Plaintiff Whittom is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

71. As a result of the Data Breach, Plaintiff Whittom anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Whittom will continue to be at increased risk of identity theft and fraud for years to come.

72. Following the Data Breach, Plaintiff Whitton provided notice and a 30-day opportunity to cure to EyeMed pursuant to Cal. Civ. Code 1798.150(b). Such notice is attached as **Exhibit C**. EyeMed did not cure the breach.

Plaintiff Wynn's Experience

73. From 2016 through 2019, Plaintiff Wynn used EyeMed for her vision care benefits. This included submitting claims to EyeMed for the purchase of prescription lenses and contact lenses from LensCrafters, Sam's Club, Apex Eye Care and Eye Concept.

74. Plaintiff Wynn entrusted her PII, PHI, and other confidential information such as contact information, health insurance policy information, prescription information, medical conditions, and Social Security number to EyeMed with the reasonable expectation and understanding that EyeMed would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have used EyeMed's services had she known that EyeMed would not take reasonable steps to safeguard her sensitive PII and PHI.

75. In December 2020, more than five months after EyeMed learned of the Data Breach, Plaintiff received a letter from EyeMed, dated December 7, 2020, notifying her that her PII and PHI had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Wynn's PII and PHI, including her full name, address, date of birth, phone number, email address, and vision insurance account/identification number, was compromised as a result of the Data Breach. A copy of the letter is attached hereto as **Exhibit D**.

76. As a result of the Data Breach, Plaintiff Wynn made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letter, including but not limited to continuing to maintain LifeLock credit monitoring that her mother, Plaintiff Tate, purchased for her. In addition, Plaintiff Wynn spent time researching the Data Breach; reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Wynn has spent approximately 35 hours since the Data Breach reviewing her bank statements and credit card accounts for irregularities. This is valuable time Plaintiff Wynn otherwise would have spent on other activities, including but not limited to work, education, and/or recreation.

77. Plaintiff Wynn suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII and PHI, a form of property that EyeMed obtained from Plaintiff Wynn; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

78. Moreover, subsequent to the Data Breach, Plaintiff Wynn also experienced actual identity theft and fraud, including fraudulent charges on both her debit and credit cards from Wells Fargo that caused her to miss out on numerous months of Wells Fargo's rewards program and

caused her to have to borrow money from relatives to pay for her college tuition because she did not have access to her funds. In addition, Plaintiff Wynn filed her state tax return and received a notification from the department of revenue that they were holding her 2020 refund until they were able to properly identify her due to fraud. Plaintiff Wynn has been notified that her private information has been found on the dark web. Plaintiff Wynn has also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages. For example, Plaintiff Wynn receives scam phone calls from different state agencies related to federal loans, medical professionals, student loans and warranty specialists daily. Plaintiff Wynn also receives emails and phone calls regarding solicitations from medical companies for medical equipment, health insurance and other medically related emails and phone calls.

79. Plaintiff Wynn has spent at least 170 hours responding to incidents related to the Data Breach and activities trying to mitigate the impact of the Data Breach. This is time Plaintiff Wynn otherwise would have spent on other activities, such as work, education, and/or recreation.

80. As a result of the Data Breach, Plaintiff Wynn has suffered emotional distress as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of identity theft and fraud. Plaintiff Wynn is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

81. As a result of the Data Breach, Plaintiff Wynn anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Wynn will continue to be at increased risk of identity theft and fraud

for years to come.

Defendant's Data Security Safeguards Were Inadequate

EyeMed Owed a Duty to Plaintiffs and Class Members to Adequately Safeguard Their PII and to Provide Timely Notice of the Data Breach

82. EyeMed is well aware of the importance of security in maintaining personal information (particularly health and medical information), and the value its users place on keeping their PII and PHI secure.

83. EyeMed owes a duty to Plaintiffs and the Class members to maintain adequate security and to protect the confidentiality of their personal data.

84. EyeMed owes a further duty to its current and former users to immediately and accurately notify them of a breach of its systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

The PII at Issue Here is Particularly Valuable to Hackers

85. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers, but credit and debit cards can be cancelled quickly mitigating the hackers' ability to cause further harm. However, information such as dates of birth and Social Security numbers are even more appealing to hackers; they are difficult to cancel, let alone change, and can be easily used to perpetrate identity theft and other types of fraud. Health information is the most valuable to hackers.[12] Indeed, according to a report by the Federal Bureau of Investigation's ("FBI") Cyber Division, healthcare records can be sold by criminals for 50 times the price of stolen Social Security numbers or credit card numbers.[13] A file containing private health insurance information such as names, phone

[12] https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited April 30, 2021).

[13] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for*

numbers, email addresses, Social Security numbers and bank account numbers with routing numbers, can be bought for between $1,200 and $1,300 each on the black market.[14]

86. Companies recognize that PII and PHI are valuable assets. Indeed, PII and PHI are valuable commodities. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other PII and PHI on a number of Internet websites. Plaintiffs' and Class members' personal data that was stolen has a high value on both legitimate and black markets.

87. Some companies recognize personal information, especially health information, as a close equivalent to personal property. Software has been created by companies to value a person's identity on the black market. The commoditization of this information is thus felt by consumers as theft of personal property in addition to an invasion of privacy. Compromised health information can lead to falsified information in medical records and fraud that can persist for years as it "is also more difficult to detect, taking twice as long as normal identity theft."[15] What is worse, a thief may use your name and health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.[16]

88. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

The use of third party information from public records, information aggregators and

---

Increased Cyber Intrusions for Financial Gain (April 8, 2014) *available at* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (last visited April 30, 2021).

[14] Elizabeth Clarke, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents* (July 15, 2013), available at https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents (last visited April 30, 2021).

[15] *See* FBI CYBER DIVISION, (U) HEALTH CARE SYSTEMS AND MEDICAL DEVICES AT RISK FOR INCREASED CYBER INTRUSIONS FOR FINANCIAL GAIN 2 (2014), *available at* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (FBI, April 8, 2014) (last visited April 30, 2021).

[16] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, *available at* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited April 30, 2021).

> even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[17]

89. Consumers rightfully place a high value not only on their PII and PHI, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[18] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII and PHI to bad actors—would be exponentially higher today. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

90. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is

[17] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited April 20, 2021).

[18] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17. Oct. 2002, *available at* https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited April 20, 2021).

> especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[19]

91. Here, the unauthorized access by the hackers left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII and PHI to mimic the identity of the user. The personal data of Plaintiffs and Class members stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiffs and the Class. Plaintiffs' and Class members' stolen personal data represents essentially one-stop shopping for identity thieves. "Not only is your social security number designed to stay with you for life, but it's interknitted with your banking and credit history. If a cyberthief has your name, address and SSN, he is not far from being able to steal your identity."[20] According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[21] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[22]

---

[19] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited April 30, 2021).

[20] *See* Susanne Rowan Kelleher quoting Charles Henderson in: *Everyone's Social Security Number Has Been Compromised. Here's How To Protect Yourself.* https://www.forbes.com/sites/suzannerowankelleher/2019/08/01/everyones-social-security-number-has-been-compromised-heres-how-to-protect-yourself/?sh=36afeafb29ac (last visited April 21, 2021).

[21] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited April 20, 2021).

[22] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

Even worse, when an identity thief takes over investment or financial accounts, the impact could affect retirement savings, mortgages, and the education of children and/or grandchildren.[23]

92. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[24] "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed, 69 percent reported feelings of fear related to personal financial safety, 60 percent reported anxiety, 42 percent reported fearing for the financial security of family members, and 8 percent reported feeling suicidal."[25]

93. More recently, the FTC has released its updated publication on protecting PII for businesses, which include instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

94. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect customers' PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent refund. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

95. As noted above, the disclosure of Social Security numbers in particular poses a

[23] *See* Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, *available at* https://www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html (last visited April 21, 2021).
[24] *Id.*
[25] *Id.*

significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[26] Former and current users of EyeMed systems whose Social Security numbers have been compromised will and already have spent time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

96. Again, because the information EyeMed allowed to be compromised and taken is of such a durable and near-permanent quality, the harms to Plaintiffs and the Class will continue to grow, and Plaintiffs and the Class will continue to be at substantial risk for further imminent and future harm.

EyeMed's Post-Breach Activity was Inadequate

97. Personal, health, and financial information can be sold on the black-market almost immediately. As Illinois Attorney General Lisa Madigan aptly put it, "the second somebody gets your credit or debit card information, it can be a matter of hours or days until it's sold on the black market and someone's starting to make unauthorized transactions."[27] Thus, the compromised information could be used weeks or even months before the receipt of any letter from EyeMed and EyeMed's proposed solutions to the potential fraud are, therefore, woefully deficient.

98. Immediate notice of a security breach is essential to protect people such as Plaintiffs and the Class members. EyeMed failed to provide such immediate notice, in fact taking at least

[26] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

[27] Phil Rosenthal, *Just assume your credit and debit card data were hacked*, http://www.chicagotribune.com/business/columnists/ct-data-breach-credit-scam-rosenthal-1001-biz-20140930-column.html#page=1 (last visited April 20, 2021).

five to six months to disclose to individual customers that there had been a breach, thus further exacerbating the damages sustained by Plaintiffs and the Class resulting from the breach.

99. Such failure to protect Plaintiffs' and the Class members' PII and PHI, and timely notify of the breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because many of the data points stolen are persistent—for example, Social Security number, name, address, email address, and medical history—as opposed to transitory—for example, the date of an appointment, criminals who purchase the PII and PHI belonging to Plaintiffs and the Class members do not need to use the information to commit fraud immediately. The PII and PHI can be used or sold for use years later.

100. A single person's PHI can fetch up to $350 on the dark web. This is due, in part, to the broad scope and comprehensive nature of the data and information, which can be used to steal identities for illegal drug or medical purchases or defraud insurers. Allowing hackers to steal this type of information is particularly nefarious, as many banks or credit card providers have substantial fraud detection systems with quick freeze or cancellation programs in place, whereas the breadth and usability of PHI allows criminals to get away with misuse for years before healthcare-related fraud is spotted.

101. Every year, victims of identity theft lose billions of dollars. And reimbursement is only the beginning, as these victims usually spend hours and hours attempting to repair the impact to their credit, at a minimum.

102. Plaintiffs and the Class members are at constant risk of imminent and future fraud, misuse of their PII and PHI, and identity theft for many years in the future as a result of the EyeMed's actions and the data breach. They have suffered real and tangible loss, including but not

limited to the loss in the inherent value of their PII and PHI, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of discovery in this case, but hitherto kept deliberately hidden by EyeMed.

CLASS ACTION ALLEGATIONS

103. Pursuant to the provisions of Rules 23(a), 23(b)(1), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure, Plaintiffs bring this class action on behalf of themselves and a nationwide class defined as:

> **All persons who reside in the United States whose personal data was compromised as a result of the Data Breach discovered by EyeMed on or about July 1, 2020 (the "Class" or "Nationwide Class").**

104. In addition, Plaintiffs Tate and Wynn seeks to represent a subclass (the "South Carolina Subclass"), defined as follows:

> **All persons who reside in South Carolina whose personal data was compromised as a result of the Data Breach discovered by EyeMed on or about July 1, 2020.**

105. In addition, Plaintiff Whittom also seeks to represent a subclass (the "California Subclass"), defined as follows:

> **All persons who reside in California whose personal data was compromised as a result of the Data Breach discovered by EyeMed on or about July 1, 2020.**

106. Excluded from the Nationwide Class and the South Carolina and California Subclasses are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

107. Plaintiffs reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

108. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

109. All members of the proposed Class are readily ascertainable in that EyeMed has access to addresses and other contact information for all members of the Class, which can be used for providing notice to Class members.

110. ***Numerosity***. The Class is so numerous that joinder of all members is impracticable. The Class includes millions of individuals whose personal data was compromised by the Data Breach.

111. ***Commonality***. There are numerous questions of law and fact common to Plaintiffs and the Class, including the following:

- whether EyeMed engaged in the wrongful conduct alleged in this Complaint;
- whether EyeMed's conduct was unlawful;
- whether EyeMed failed to implement and maintain reasonable systems and security procedures and practices to protect customers' personal data;
- whether EyeMed unreasonably delayed in notifying affected customers of the Data Breach;
- whether EyeMed owed a duty to Plaintiffs and members of the Class to adequately protect their personal data and to provide timely and accurate notice of the EyeMed Data Breach to Plaintiffs and members of the Class;
- whether EyeMed breached its duties to protect the personal data of Plaintiffs and

members of the Class by failing to provide adequate data security and failing to provide timely and adequate notice of the EyeMed Data Breach to Plaintiffs and the Class;

- whether EyeMed's conduct was negligent;
- whether EyeMed knew or should have known that its computer systems were vulnerable to attack;
- whether EyeMed's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of its systems, resulting in the loss of Class members' personal data;
- whether EyeMed wrongfully or unlawfully failed to inform Plaintiffs and members of the Class that it did not maintain computers and security practices adequate to reasonably safeguard customers' financial and personal data;
- whether EyeMed should have notified the public, Plaintiffs, and Class members immediately after it learned of the Data Breach;
- whether Plaintiffs and members of the Class suffered injury, including ascertainable losses, as a result of EyeMed's conduct (or failure to act);
- whether Plaintiffs and members of the Class are entitled to recover damages; and
- whether Plaintiffs and Class members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

112. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class members, had their personal data compromised, breached and stolen in the EyeMed Data Breach. Plaintiffs and all Class members were injured through the uniform misconduct of

EyeMed described in this Complaint and assert the same claims for relief.

113. ***Adequacy***. Plaintiffs and counsel will fairly and adequately protect the interests of the Class. Plaintiffs have retained counsel who are experienced in Class action and complex litigation. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other members of the class.

114. ***Predominance***. The questions of law and fact common to Class members predominate over any questions which may affect only individual members.

115. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, EyeMed's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class members have been harmed by EyeMed's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to EyeMed's conduct and/or inaction. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for EyeMed. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary,

causing EyeMed to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because EyeMed has acted and failed and refused to act in a manner that generally applies to all Class members' PII and PHI in a manner, so final injunctive relief is appropriate with regard to the Class as a whole.

COUNT I
Negligence

116. Plaintiffs incorporate all other allegations in the Complaint as if fully set forth herein.

117. EyeMed required Plaintiffs and Class members to submit non-public PII and PHI to obtain medical service benefits.

118. By collecting, storing, and using Plaintiffs' and Class members' PII and PHI, EyeMed owed a duty to Plaintiffs and members of the Class to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII and PHI that they were required to provide EyeMed as a condition of receiving EyeMed's services from being compromised, lost, stolen, accessed and misused by unauthorized persons. EyeMed was required

to prevent foreseeable harm to Plaintiffs and the Class members, and therefore had a duty to take reasonable steps to safeguard sensitive PII and PHI from unauthorized release or theft. More specifically, this duty included: (1) designing, maintaining, and testing EyeMed's data security systems and data storage architecture to ensure Plaintiffs' and Class members' PII and PHI were adequately secured and protected: (2) implementing processes that would detect an unauthorized breach of EyeMed's security systems and data storage architecture in timely and adequate manner; (3) timely acting on all warnings and alerts, including public information, regarding EyeMed's security vulnerabilities and potential compromise of the PII and PHI of Plaintiffs and Class members; (4) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements; and (5) timely and adequately informing Plaintiffs and Class members if and when a data breach occurred to prevent foreseeable harm to them, notwithstanding undertaking (1)-(4) above.

119. EyeMed had a common law duty to prevent foreseeable harm to Plaintiffs and Class members. The duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices at EyeMed in its affirmative collection of PII and PHI from Plaintiffs and Class members. In fact, not only was it foreseeable that Plaintiffs and Class members would be harmed by the failure to protect their PII and PHI because hackers routinely attempt to steal such information for use in nefarious purposes, EyeMed knew that it was more likely than not Plaintiffs and Class members would be harmed as a result.

120. EyeMed's duties to use reasonable security measures also arose as a result of the special relationship that existed between it, on the one hand, and Plaintiffs and Class members, on the other hand. This special relationship recognized in laws and regulations, arose because Plaintiffs and Class members entrusted EyeMed with their PII and PHI by virtue of receiving

health benefits through EyeMed. EyeMed alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

121. EyeMed's duties of care also arose under the California Unfair Competition Law, the California's Confidentiality of Medical Information Act ("CMIA"), and the California Consumer Privacy Act ("CCPA").

122. There is a very close connection between EyeMed's failure to follow reasonable security standards to protect its current and former users' personal data and the injury to Plaintiffs and the Class. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

123. If EyeMed had taken reasonable security measures, data thieves would not have been able to take the personal information of millions of current and former users of EyeMed's services. The policy of preventing future harm weighs in favor of finding a special relationship between EyeMed and Plaintiffs and the Class. If companies are not held accountable for failing to take reasonable security measures to protect their customers' personal data, they will not take the steps that are necessary to protect against future security breaches.

124. EyeMed owed a duty to timely disclose the material fact that EyeMed's computer systems and data security practices were inadequate to safeguard users' personal, health, and financial data from theft.

125. EyeMed breached these duties by the conduct alleged in the Complaint by, including without limitation, failing to protect its customers' personal, health, and financial, information; failing to maintain adequate computer systems and data security practices to

safeguard customers' personal, health, and financial information; allowing unauthorized access to Plaintiffs' and Class members' PII and PHI; failing to disclose the material fact that EyeMed's computer systems and data security practices were inadequate to safeguard customers' personal, health, and financial data from theft; and failing to disclose in a timely and accurate manner to Plaintiffs and members of the Class the material fact of the data breach.

126. But for EyeMed's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, their PII and PHI would not have been compromised. Specifically, as a direct and proximate result of EyeMed's failure to exercise reasonable care and use commercially reasonable security measures, the personal data of current and former EyeMed users was accessed by ill-intentioned criminals who could and will use the information to commit identity or financial fraud. Plaintiffs and the Class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

127. It was foreseeable that (1) EyeMed's failure to safeguard the PII and PHI of Plaintiffs and Class members would lead to one or more types of injury to them; and (2) data breach at EyeMed was foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

128. As a proximate result of this conduct, Plaintiffs and the other class members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Such injuries include those described above, including one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of value of their privacy and confidentiality of the compromised PII and PHI; illegal sale of the compromised PII and PHI on

the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card, statements, insurance statements, credit reports; expenses and time spent initiating fraud alerts, decreased credit scores and ratings; lost time; lost value of PII and PHI; other economic harm; and emotional distress as a result of the Data Breach.

COUNT II
Negligence Per Se

129. Plaintiffs incorporate all other allegations in the Complaint as if fully set forth herein.

130. Pursuant to the FTC Act, 15 U.S.C. § 45, EyeMed had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and Class members.

131. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of EyeMed's duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

132. Pursuant to HIPAA, EyeMed had a duty to implement reasonable safeguards to protect Plaintiffs' and Class members' PII. *See* 42 U.S.C. § 1302(d), *et seq.*

133. Pursuant to HIPAA, EyeMed had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." 45 C.F.R. §164.304.

134. Pursuant to the Gramm-Leach-Bliley Act, EyeMed had a duty to protect the security and confidentiality of Plaintiffs' and Class members' PII. *See* 15 U.S.C. § 6801.

135. Pursuant to the FCRA, EyeMed had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiffs' and Class members' PII. *See* 15 U.S.C. § 1681(b).

136. EyeMed's duties to use reasonable data security measures also arose under the CCPA, Cal. Civ. Code § 1798.100, *et seq.*, which imposes a "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

137. Pursuant to the CMIA, Cal. Civ. Code § 56, *et seq.*, EyeMed had a statutory duty to, among other things, protect and preserve the integrity of electronic medical information. *See* Cal. Civ. Code §§ 56.06, 56.101(a), 56.101(b)(1)(A).

138. EyeMed's duties to use reasonable data security measures also arose under the California Customer Records Act ("CCRA"), Cal. Civ. Code § 1798.80, *et seq.*, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

139. Pursuant to the UCL, EyeMed had duty to provide fair and adequate computer systems and data security to safeguard the PII and PHI of Plaintiffs and Class members. *See* Cal. Bus. & Prof. Code §§ 17200, *et seq.*

140. EyeMed solicited, gathered, and stored PII and PHI of Plaintiffs and the Class members to facilitate transactions which affect commerce.

141. EyeMed violated the FTC Act (and similar state statutes), the CCPA, CCRA, CMIA, HIPAA, the FCRA, and the Graham-Leach-Bliley Act by failing to use reasonable measures to protect PII and PHI of Plaintiffs and Class members and not complying with applicable industry standards, as described herein. EyeMed's conduct was particularly unreasonable given the nature and amount of PII and PHI obtained and stored and the foreseeable consequences of a data breach on EyeMed's systems.

142. EyeMed's violation of the FTC Act (and similar state statutes) as well as its violations of the CCPA, CMIA, CCRA, HIPAA, the FCRA, and the Graham-Leach-Bliley Act constitutes negligence *per se*.

143. Plaintiffs and the Class members are within the class of persons that the FTC Act (and similar state statutes), HIPAA, the FCRA, and the Graham-Leach-Bliley Act were intended to protect. Plaintiff Whittom and the California Subclass members are within the class of persons that the CCPA, CMIA, and CCRA were intended to protect.

144. The harm that occurred as a result of the breach is the type of harm the FTC Act (and similar state statutes), as well as the CCPA, CMIA, CCRA, HIPAA, the FCRA, and the Graham-Leach-Bliley Act were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiffs and the Class members.

145. As a direct and proximate result of EyeMed's negligence *per se*, Plaintiffs and Class members have suffered, and continue to suffer, damages arising from the breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

146. Such injuries include one or more of the following: ongoing, imminent, certainly

impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by EyeMed, reviewing bank statements, payment card statements, provider and insurance statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; and other economic and non-economic harm.

COUNT III
Breach of Implied Contract

147. Plaintiffs incorporate all other allegations in the Complaint as if fully set forth herein.

148. Plaintiffs and the Class delivered their personal, health, and financial information to EyeMed as part of the process of obtaining services provided by EyeMed.

149. Plaintiffs and members of the Class entered into implied contracts with EyeMed under which EyeMed agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class members that their data had been breached and compromised.

150. In providing such data, Plaintiffs and the other members of the Class entered into an implied contract with EyeMed whereby EyeMed became obligated to reasonably safeguard Plaintiffs' and the other Class members' sensitive, non-public information.

151. In delivering their personal data to EyeMed, Plaintiffs and Class members intended and understood that EyeMed would adequately safeguard their personal data.

152. Plaintiffs and the Class members would not have entrusted their private and confidential financial, health, and personal information to Defendants in the absence of such an implied contract.

153. EyeMed accepted possession of Plaintiffs' and Class members' personal data for the purpose of providing services to Plaintiffs and Class members.

154. Had EyeMed disclosed to Plaintiffs and members of the Class that EyeMed did not have adequate computer systems and security practices to secure users' and former users' personal data, Plaintiffs and members of the Class would not have provided their PII and PHI to EyeMed.

155. EyeMed recognized that its users' and former users' personal data is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and members of the Class.

156. Plaintiffs and members of the Class fully performed their obligations under the implied contracts with EyeMed.

157. EyeMed breached the implied contract with Plaintiffs and the other members of the Class by failing to take reasonable measures to safeguard their data.

158. As a proximate result of this conduct, Plaintiffs and the other Class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
Unjust Enrichment

159. Plaintiffs incorporate all other allegations in the Complaint as if fully set forth herein.

160. Plaintiffs and Class members conferred a monetary benefit on EyeMed in the form of monies or fees paid for services from EyeMed. EyeMed had knowledge of this benefit when it accepted the money from Plaintiffs and the Class members.

161. The monies or fees paid by the Plaintiffs and Class members were supposed to be used by EyeMed, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiffs and Class members.

162. EyeMed failed to provide reasonable security, safeguards, and protections to the personal data of Plaintiffs and Class members, and as a result the Plaintiffs and Class overpaid EyeMed as part of services they purchased.

163. EyeMed failed to disclose to Plaintiffs and members of the Class that its computer systems and security practices were inadequate to safeguard users' and former users' personal data against theft.

164. Under principles of equity and good conscience, EyeMed should not be permitted to retain the money belonging to Plaintiffs and Class members because EyeMed failed to provide adequate safeguards and security measures to protect Plaintiffs' and Class members' personal, health, and financial information that they paid for but did not receive.

165. EyeMed wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class members.

166. EyeMed's enrichment at the expense of Plaintiffs and Class members is and was unjust.

167. As a result of EyeMed's wrongful conduct, as alleged above, Plaintiffs and the Class are entitled under the unjust enrichment laws of all 50 states and the District of Columbia to restitution and disgorgement of all profits, benefits, and other compensation obtained by EyeMed, plus attorneys' fees, costs, and interest thereon.

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

168. Plaintiff Whittom incorporates all other allegations in the Complaint as if fully set forth herein.

169. EyeMed is a "person" as defined by Cal. Bus. & Prof. Code § 17201. EyeMed violated California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

170. In the ordinary course of its business, EyeMed required Plaintiff Whittom and California Subclass members to provide it with sensitive PII and PHI, but it promised that in doing so, it was "committed to protecting [members'] privacy," and would "safeguard" the PII. But Defendant failed to have adequate data security measures in place, and thus failed to adequately ensure the privacy, confidentiality, and security of PII data that Plaintiff Whittom and Subclass members entrusted to it

171. EyeMed's unlawful, unfair, and deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Whittom and California Subclass members' PII, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the healthcare sector, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Whittom and California Subclass members' PII, including duties

imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Whittom and California Subclass members' PII and PHI, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Whittom and California Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and CCRA, Cal. Civ. Code § 1798.80, *et seq.*; CMIA, Cal. Civ. Code § 56, *et seq.*, and CCPA, Cal. Civ. Code § 1798.100 *et seq.*;

(f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Whittom and California Subclass members' PII and PHI; and

(g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Whittom and California Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. §4 5; CCRA, Cal. Civ. Code § 1798.80, *et seq.*; CMIA, Cal. Civ. Code § 56, *et seq*, and CCPA, Cal. Civ. Code § 1798.100, *et seq.*

172. EyeMed's actions and practices as described above constitute "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiff Whittom and the California Subclass members outweighs the utility of EyeMed's conduct, as separately, violated fundamental California public policy. This conduct includes EyeMed'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.

EyeMed engaged in unfair business practices under the "balancing test."

173. The harm caused by EyeMed's actions and omissions, as described above, greatly outweighs any perceived utility. EyeMed's failure to follow basic data security cannot be said to have had any utility at all. For example, there was no utility in EyeMed telling Plaintiff Whittom and the California Subclass members that it promises to "[m]aintain the privacy and safeguard the security of your health information"[28] because it did not take adequate steps to do so. And there was no utility in Defendant promising that if it discovers 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"[29] because it had a breach occur and did not in fact, give notice of the breach within 60 days. Each of these actions and omissions was clearly injurious to Plaintiff Whittom and the California Subclass Members, directly causing the harms alleged.

EyeMed engaged in unfair business practices under the "tethering test."

174. EyeMed's actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.,* Cal. Civ. Code § 1978.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them…. The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1978.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents be protected."). Defendants' acts and omissions, and the injuries caused by them are thus "comparable to or the same as a violation of the law . . ." *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal. 4th 163, 187 (1999).

[28] https://eyemed.com/en-us-hipaa-notice-of-privacy-practices (last visited April 30, 2021).
[29] *Id.*

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

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

177. Accordingly, Plaintiff Whittom 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 EyeMed; 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 V
Violations of California's Confidentiality of Medical Information Act
Cal. Civ. Code § 56, et seq. ("CMIA")
On Behalf of Plaintiff Whittom and the California Subclass

178. Plaintiff Whittom incorporates all other allegations in the Complaint as if fully set forth herein.

179. EyeMed 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).

180. Plaintiff Whittom and California Subclass members are "enrollees" and/or "subscribers" of EyeMed 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 Whittom 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, when Defendant discovered the data breach.

181. EyeMed negligently created, maintained, preserved, stored, and then exposed Plaintiff Whittom'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.

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

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

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

185. Plaintiff Whittom'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).

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

187. As a result of EyeMed's above-described conduct, Plaintiff Whittom 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.

188. As a direct and proximate result of EyeMed'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 Whittom 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.

189. Plaintiff Whittom, individually and for each member of the California Subclass, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2).

COUNT VI
Violations of California Consumer Privacy Act,
Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA")
On Behalf of Plaintiff Whittom and the California Subclass

190. Plaintiff Whittom incorporates by reference all other allegations in the Complaint as if fully set forth herein.

191. Plaintiff Whitton and California Subclass members are "consumer[s]" as that term is defined in Cal. Civ. Code. § 1798.140(g).

192. EyeMed is a "business" as that term is defined in Cal. Civ. Code. § 1798.140(c). As set forth above, EyeMed is a corporation organized or operated for the profit or financial benefit of its shareholders or other owners. EyeMed does business in the State of California. EyeMed collects consumers' (including Plaintiff's and California Subclass members') personal information and determines the purposes and means of the processing of this personal information (*e.g.*, it designs the systems that process and store consumers' personal information). EyeMed annually receives for the business's commercial purposes or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers.

193. Plaintiff Whittom and California Subclass members' PII is "nonencrypted and nonredacted personal information" as that term is used in Cal. Civ. Code § 1798.150(a)(1). At a minimum, this PII included the individual's first name or first initial and last name, in combination with medical information and health insurance information. In some instances, the PII also included Social Security numbers, financial information, and unique identification numbers issued on government documents (*e.g.*, driver's license numbers).

194. The Data Breach constitutes "an unauthorized access and exfiltration, theft, or disclosure" pursuant to Cal. Civ. Code § 1798.150(a)(1).

195. EyeMed had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the Plaintiff's and California Subclass members' PII to protect said PII.

196. EyeMed breached the duty it owed to Plaintiff Whittom and California Subclass members described above. EyeMed breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff Whittom and California Subclass members; (b) detect the Data Breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

197. EyeMed's breach of the duty it owed to Plaintiff Whittom and California Subclass members described above was the direct and proximate cause of the Data Breach. As a result, Plaintiff Whittom and California Subclass members suffered damages, as described above and as will be proven at trial.

198. Plaintiff Whittom seeks injunctive relief in the form of an order enjoining EyeMed from continuing the practices that constituted its breach of the duty owed to Plaintiff and California Subclass members as described above.

199. Plaintiff Whittom also seeks statutory damages, actual damages, and all other forms of relief available under the CCPA.

200. Plaintiff Whittom served EyeMed with a notice of claim under the CCPA on December 22, 2020, pursuant to Cal. Civ. Code. § 1798.150(b). *See* **Exhibit C**. As of the filing date of this Consolidated Complaint, Plaintiff Whittom has received no satisfactory response from EyeMed.

RELIEF REQUESTED

Plaintiffs, individually and on behalf of the proposed Class, requests that the Court:

1. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiffs as Class representatives, and appoint the undersigned counsel as class counsel;
2. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and other Class members;
3. Award restitution; compensatory, consequential, and general damages, including nominal damages as allowed by law in an amount to be determined at trial;
4. Award statutory damages to Plaintiffs and Class members in an amount to be determined at trial;
5. Award Plaintiffs and Class members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;
6. Award Plaintiffs and Class members pre- and post-judgment interest, to the extent allowable; and
7. Award such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable as of right.

Respectfully submitted,

/s/ Terence R. Coates
W.B. Markovits (0018514)
Terence R. Coates (0085579)
Zachary C. Schaengold (0090953)
Dylan J. Gould (0097954)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650

Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
bmarkovits@msdlegal.com
tcoates@msdlegal.com
zschaengold@msdlegal.com
dgould@msdlegal.com

Liaison Counsel for Plaintiffs and the Class

Bryan L. Bleichner (*pro hac vice)*
Jeffrey D. Bores (*pro hac vice)*
Christopher P. Renz (*pro hac vice)*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
jbores@chestnutcambronne.com
crenz@chestnutcambronne.com

Lori G. Feldman (*pro hac vice*)
GEORGE GESTEN MCDONALD, PLLC
102 Half Moon Bay Drive
Croton- On-Hudson, NY 10502
Phone: (917) 983-9321
Fax: (888) 421-4173
LFeldman@4-Justice.com

David J. George *(pro hac vice)*
Brittany L. Brown (*pro hac vice*)
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite 302
Lake Worth, FL 33463
Phone: (561) 232-6002
Fax: (888) 421-4173
DGeorge@4-Justice.com
BBrown@4-Justice.com

Co-Lead Counsel for Plaintiffs and the Class

Gayle M. Blatt (*pro hac vice)*
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street

San Diego, CA 92101
Phone: (619)238-1811
gmb@cglaw.com

Executive Committee for Plaintiffs and the Class

Melissa R. Emert (*pro hac* vice)
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
747 Chestnut Ridge Road
Chestnut Ridge, NY 10977
Tel: (866) 680-1835
memert@kgglaw.com

Executive Committee for Plaintiffs and the Class

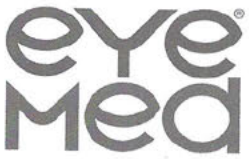
CERTIFICATE OF SERVICE

The undersigned hereby certifies that on April 30, 2021, the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ Terence R. Coates
Terence R. Coates (0085579)

EXHIBIT

A



21 1 6984 **********AUTO**5-DIGIT 29016
CHANDRA PRICE
[redacted]

December 7, 2020

RE: Security Incident

Dear Chandra Price,

EyeMed manages vision benefits on behalf of your current or former employer. EyeMed takes the privacy and confidentiality of your information very seriously. We write to inform you of a data security incident that may have involved some of your personal information. This notice explains the incident, measures we have taken, and steps you can take in response.

What happened?

On July 1, 2020, EyeMed discovered that an unauthorized individual gained access to an EyeMed email mailbox and sent phishing emails to email addresses contained in the mailbox's address book. On the same day, EyeMed took immediate action to block the unauthorized individual's access to the mailbox and secured the mailbox. EyeMed immediately launched an investigation into the incident and engaged a cybersecurity firm to assist in its efforts. It was determined that the unauthorized individual first gained access to the mailbox on June 24, 2020, and that access terminated on July 1, 2020.

What information was involved?

The mailbox contained information about individuals who formerly or currently receive vision benefits through EyeMed. Although EyeMed could not fully determine whether, and to what extent, if any, the unauthorized individual viewed or copied personal information, it is possible that personal information was viewed or acquired by the unauthorized individual.

Following a detailed analysis and review of all potentially compromised emails and files, EyeMed identified the names of all individuals who were impacted, as well as the type of information included in those files. Personal information that may have been accessed could include the following types of information: full name, address, date of birth, phone number, email address, and vision insurance account/identification number.

What we are doing:

EyeMed is committed to safeguarding your personal information and has taken immediate steps to enhance the protections that were already in place before this incident. In addition to the investigation, EyeMed made changes to how authorized individuals access the EyeMed network and required immediate complex password changes to all our employee accounts. EyeMed is also reinforcing and providing additional mandatory security awareness training.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **April 1, 2021** to activate your identity monitoring services.*

Membership Number: [redacted]

Additional information describing your identity monitoring services is included with this letter.

What you can do:

EyeMed is not aware of any misuse of your information. However, we want to let you know of steps you may want to take to guard against potential identity theft or fraud. We encourage you to remain vigilant by regularly reviewing your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity. If you identify services that you did not receive or accounts, charges, or withdrawals that you did not authorize, you should immediately contact and report to the involved company and to credit reporting agencies.

Please also review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

More Information:

If you have questions, please call 1-888-974-0076, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Sincerely,

Jason Groppe

Jason D. Groppe
Chief Privacy Officer (N.A.)

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a security freeze for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

EXHIBIT

B

240 2 76369 **********AUTO**ALL FOR AADC 945
BARBARA SMITH WHITTOM
[redacted]

November 27, 2020

Re: Notice of Data Breach

Dear Barbara Smith Whittom,

EyeMed manages vision benefits on behalf of your carrier. EyeMed takes the privacy and confidentiality of your information very seriously. We write to inform you of a data security incident that may have involved some of your personal information. This notice explains the incident, measures we have taken, and steps you can take in response.

What happened?

On July 1, 2020, EyeMed discovered that an unauthorized individual gained access to an EyeMed email mailbox and sent phishing emails to email addresses contained in the mailbox's address book. On the same day, EyeMed took immediate action to block the unauthorized individual's access to the mailbox and secured the mailbox. EyeMed immediately launched an investigation into the incident and engaged a cybersecurity firm to assist in its efforts. It was determined that the unauthorized individual first gained access to the mailbox on June 24, 2020, and that access terminated on July 1, 2020.

What information was involved?

The mailbox contained information about individuals who formerly or currently receive vision benefits through EyeMed. Although EyeMed could not fully determine whether, and to what extent, if any, the unauthorized individual viewed or copied personal information, it is possible that personal information was viewed or acquired by the unauthorized individual.

Following a detailed analysis and review of all potentially compromised emails and files, EyeMed identified the names of all individuals who were impacted, as well as the type of information included in those files. Personal information that may have been accessed could have included the following types of information: full name, address, date of birth, full or partial social security number, Health Insurance/Member ID Number, and/or other personal or financial information.

What we are doing:

EyeMed is committed to safeguarding your personal information and has taken immediate steps to enhance the protections that were already in place before this incident. In addition to the investigation, EyeMed made changes to how authorized individuals access the EyeMed network and required immediate complex password changes to all our employee accounts. EyeMed is also reinforcing and providing additional mandatory security awareness training.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **April 1, 2021** to activate your identity monitoring services.*

Kroll Membership Number: [redacted]

Additional information describing your identity monitoring services is included with this letter.

[redacted]

ELN-4695-1120 -76369

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a security freeze for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What you can do:

EyeMed is not aware of any misuse of your information. However, we want to let you know of steps you may want to take to guard against potential identity theft or fraud. We encourage you to remain vigilant by regularly reviewing your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity. If you identify services that you did not receive or accounts, charges, or withdrawals that you did not authorize, you should immediately contact and report to the involved company and to credit reporting agencies.

Please also review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

More Information:

If you have questions, please call 1-844-480-0273, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your Kroll membership number ready.

Sincerely,

Jason Groppe

Jason D. Groppe
Chief Privacy Officer (N.A.)

EXHIBIT

C

CaseyGerry

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD LLP

110 Laurel Street, San Diego, CA 92101-1419
Tel (619) 238-1811 Fax (619) 544-9232

David S. Casey, Jr.
Frederick Schenk
Robert J. Francavilla
Gayle M. Blatt
Thomas D. Luneau
Jeremy K. Robinson
Jason C. Evans
P. Camille Guerra*
Srinivas Hanumadass
Adam B. Levine
Meagan L. Verschueren
Jillian F. Hayes
David S. Casey III
James M. Davis

of Counsel
Thomas D. Penfield
Scott C. Cummins
Angela Jae Chun

David S. Casey, Sr.
1913-2003
President,
California State Bar, 1975

Richard F. Gerry
1924-2004
President,
Association of Trial Lawyers of America, 1982

David S. Casey, Jr.
President,
Association of Trial Lawyers of America, 2004

*Also Admitted in New Mexico

North County Office
1901 Camino Vida Roble, Ste. 121
Carlsbad, CA 92008

December 22, 2020

EyeMed Vision Care, LLC
National Registered Agents, Inc.
4400 Easton Commons Way, Suite 125
Columbus, Ohio 43219

Re: *Whittom v. EyeMed Vision Care, LLC*

Please take notice that this letter constitutes notice under the California Consumer Privacy Act ("CCPA"), California Civil Code section 1798.100, et seq. Pursuant specifically to Civil Code section 1798.150(b), we are hereby notifying EyeMed Vision Care, LLC ("EyeMed") of the violation of the CCPA and of our demand that, to the extent any cure exists, you cure such violation within thirty (30) calendar days from your receipt of this letter.

Plaintiff Barbara Whittom is a resident of California whose personal identifying information ("PII"), including full name, address, date of birth, full or partial social security number, Health Insurance/Member ID number, and/or other personal or financial information was accessed as a result of an unauthorized individual hacking one or more of EyeMed's email accounts. Plaintiff Whittom received a notice from EyeMed informing her that the PII she had provided to EyeMed was no longer secure.

Please be advised that EyeMed's failure to prevent Plaintiff's and other California customers' nonredacted and nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of your violation of your duty to implement and maintain reasonable security procedures and practices amounts to a violation of the CCPA, Civil Code section 1798.150. The failure includes the lack of adequate data security to prevent an unauthorized individual(s) from accessing EyeMed's email accounts.

CaseyGerry

We hereby request that EyeMed immediately cure the violation of the CCPA which exposed Plaintiff's and other California consumers' nonredacted and nonencrypted PII, to the extent there is any possible cure. Please be advised that your failure to comply with this request within thirty (30) calendar days may subject you to statutory damages on an individual and/or class-wide basis.

I look forward to discussing this matter with you. Thank you for your courtesy and cooperation.

Sincerely yours,

/s/ Gayle M. Blatt
GAYLE M. BLATT

EXHIBIT

D

21 1 6916 **********AUTO**5-DIGIT 29016
ALEXUS WYNN
[redacted]

December 7, 2020

RE: Security Incident

Dear Alexus Wynn,

EyeMed manages vision benefits on behalf of your current or former employer. EyeMed takes the privacy and confidentiality of your information very seriously. We write to inform you of a data security incident that may have involved some of your personal information. This notice explains the incident, measures we have taken, and steps you can take in response.

What happened?

On July 1, 2020, EyeMed discovered that an unauthorized individual gained access to an EyeMed email mailbox and sent phishing emails to email addresses contained in the mailbox's address book. On the same day, EyeMed took immediate action to block the unauthorized individual's access to the mailbox and secured the mailbox. EyeMed immediately launched an investigation into the incident and engaged a cybersecurity firm to assist in its efforts. It was determined that the unauthorized individual first gained access to the mailbox on June 24, 2020, and that access terminated on July 1, 2020.

What information was involved?

The mailbox contained information about individuals who formerly or currently receive vision benefits through EyeMed. Although EyeMed could not fully determine whether, and to what extent, if any, the unauthorized individual viewed or copied personal information, it is possible that personal information was viewed or acquired by the unauthorized individual.

Following a detailed analysis and review of all potentially compromised emails and files, EyeMed identified the names of all individuals who were impacted, as well as the type of information included in those files. Personal information that may have been accessed could include the following types of information: full name, address, date of birth, phone number, email address, and vision insurance account/identification number.

What we are doing:

EyeMed is committed to safeguarding your personal information and has taken immediate steps to enhance the protections that were already in place before this incident. In addition to the investigation, EyeMed made changes to how authorized individuals access the EyeMed network and required immediate complex password changes to all our employee accounts. EyeMed is also reinforcing and providing additional mandatory security awareness training.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **April 1, 2021** to activate your identity monitoring services.*

Membership Number: [redacted]

Additional information describing your identity monitoring services is included with this letter.

What you can do:

EyeMed is not aware of any misuse of your information. However, we want to let you know of steps you may want to take to guard against potential identity theft or fraud. We encourage you to remain vigilant by regularly reviewing your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity. If you identify services that you did not receive or accounts, charges, or withdrawals that you did not authorize, you should immediately contact and report to the involved company and to credit reporting agencies.

Please also review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

More Information:

If you have questions, please call 1-888-974-0076, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Sincerely,

Jason Groppe

Jason D. Groppe
Chief Privacy Officer (N.A.)

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a security freeze for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.