Adam E. Polk (State Bar No. 273000)
Simon Grille (State Bar No. 294914)
Jordan N. Isern (State Bar No. 343159)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: sgrille@girardsharp.com
Email: apolk@girardsharp.com
Email: jisern@girardsharp.com

Counsel for Plaintiff and the Proposed Class

SUPERIOR COURT FOR THE STATE OF CALIFORNIA
COUNTY OF ALAMEDA

23CV057175

PATRICK LEW, on behalf of himself and all others similarly situated,

Plaintiff,

v.

CALIFORNIA PHYSICIANS' SERVICE d/b/a BLUE SHIELD OF CALIFORNIA and MEDICAL EYE SERVICES, INC.,

Defendants.

CLASS ACTION COMPLAINT

1. Negligence;
2. Violation of the California Consumer Privacy Act of 2018, Civ. Code § 1798.100 *et seq.*;
3. Violation of the California Confidentiality of Medical Information Act, Civ. Code § 56 *et seq.*;
4. Violation of the California Customer Records Act, Civ. Code § 1798.80 *et seq.*;
5. Violation of the Unfair Competition Law, Bus. & Prof. Code § 17200 *et seq.*; and
6. Invasion of Privacy

DEMAND FOR JURY TRIAL

Plaintiff Patrick Lew ("Plaintiff"), individually and on behalf of the proposed class defined below, brings this action against Defendants California Physicians' Service d/b/a Blue Shield of California ("Blue Shield") and Medical Eye Services, Inc. ("MESVision"), and alleges as follows:

I. SUMMARY OF THE ACTION

85. Defendants neglected to secure highly sensitive personal information of Blue Shield members and beneficiaries, which resulted in a data breach that compromised their personally identifiable information ("PII") and personal health information ("PHI").

86. Blue Shield uses MESVision—a vision benefits administrator—to manage vision benefits for many Blue Shield members and beneficiaries. On May 28 and 31, a ransomware gang exfiltrated Blue Shield members and beneficiaries' sensitive data through a vulnerability in MESVision's file transfer software (the "Data Breach" or "Breach"). MESVision detected the Data Breach on August 23, and notified Blue Shield of the breach on September 1, 2023. MESVision and Blue Shield then waited another 11 weeks to notify potentially impacted members and beneficiaries, on November 14, 2023, and November 10, 2023, respectively.

87. According to Bill Budington, senior staff technologist at the Electronic Frontier Foundation, "[t]ypically 'highly sensitive information' like the data stolen from Blue Shield ends up for sale on the illicit online marketplace known as the darkweb."

88. Now, Plaintiff and other members of the proposed class must deal with the fallout. The attack exposed over 600,000 individuals' PII and PHI in total. For impacted members and beneficiaries, PII and PHI stolen in the Data Breach includes (but is not limited to) member name, member date of birth, address, subscriber ID number, subscriber name, subscriber date of birth, subscriber Social Security number, group ID number, vision provider's name, patient ID number, vision claims number, vision related treatment and diagnosis information, and vision related treatment cost information.

89. Plaintiff's information continues to reside on or remain accessible through Defendants' systems. Plaintiff by this action seeks compensatory and statutory damages as well as injunctive relief to remediate Defendants' deficient cybersecurity and provide credit

monitoring, identity theft insurance, and credit repair services (or the money needed to secure those services) to protect him and the other breach victims from identity theft and fraud.

II. PARTIES

90. Plaintiff Patrick Lew is a citizen and resident of San Francisco County.

91. Defendant California Physicians' Service d/b/a Blue Shield of California is a mutual benefit corporation headquartered in Alameda County.

92. Defendant Medical Eye Services, Inc. is a California corporation headquartered in Orange County.

III. JURISDICTION AND VENUE

93. This Court has jurisdiction over this action under section 410.10 of the California Code of Civil Procedure and Article VI, section 10 of the California Constitution.

94. This Court has personal jurisdiction over Defendants because they are headquartered in and have their principal places of business in California.

95. Venue is proper in this Court under Code of Civil Procedure sections 395 and 395.5 because Defendant Blue Shield is headquartered in this county and a substantial part of the acts or omissions giving rise to this action occurred in this county.

IV. FACTUAL ALLEGATIONS

Plaintiff's PII and PHI was compromised in the Data Breach

Plaintiff Lew

96. Plaintiff Lew is a member of Blue Shield with health insurance benefits administered by MESVision. In order to receive treatment and other health care services, Plaintiff Lew provided personally identifying information, including his name, social security number, address, e-mail address, and telephone number. He also provided information concerning his medical history, mental or physical condition, and treatment history.

97. On November 10, 2023, Plaintiff Lew received a letter from Blue Shield informing him of the Data Breach and advising him to take protective measures. The letter also informed him that his name, date of birth, address, subscriber ID, group ID number, and social security number, may have been subject to the data breach.

98. The exposure of his private and confidential information, including health information, in the Data Breach has caused Plaintiff Lew to suffer stress related to his personal information being compromised and to devote more time to checking his credit reports and financial accounts for fraudulent activity. Plaintiff Lew has increased concerns over the loss of his privacy.

Background regarding MESVision and Blue Shield

99. Blue Shield is a California-based mutual benefit corporation and health plan provider with over 4.8 million members.[1] Among the plans it provides, Blue Shield provides vision plans that offers access to vision providers in California.[2] All Blue Shield vision plans are administered by MESVision.[3]

100. MESVision is a California-based vision benefit program provider and administrator who provides administration services to all Blue Shield vision benefit plans.[4] It also receives the PII and PHI of members and beneficiaries related to member eligibility, authorized third parties, and vision claims processing.[5] This information includes, but is not limited to, member name, member date of birth, address, subscriber ID number, subscriber name, subscriber date of birth, subscriber Social Security number, group ID number, vision provider's

---

[1] https://news.blueshieldca.com/about#:~:text=Blue%20Shield%20of%20California%20is,%2424%20billion%20in%20annual%20revenue. (last accessed Dec. 6, 2023).

[2] https://www.blueshieldca.com/bsca/bsc/wcm/connect/broker/broker_content_unauth_en/ifp/vision/home (last accessed Dec. 6, 2023).

[3] https://www.blueshieldca.com/bsca/bsc/wcm/connect/member/member_content_en/content%20root/ifp/plan_resources/your_vision_plan (last accessed Dec. 6, 2023).

[4] https://www.blueshieldca.com/bsca/bsc/wcm/connect/member/member_content_en/content%20root/ifp/plan_resources/your_vision_plan#:~:text=Blue%20Shield%20vision%20plans%20are,and%20are%20administered%20by%20MESVision. (last accessed Dec. 6, 2023).

[5] https://www.healthcarefinancenews.com/news/data-breach-hits-blue-shield-california (last accessed Dec. 6, 2023).

name, patient ID number, vision claims number, vision related treatment and diagnosis information, and vision related treatment cost information.[6]

101. MESVision used file transfer software to send and receive files.[7] MESVision represents, "all transactions occur through our secure server."[8] Further, MESVision's HIPAA Notice represents, its vision plan beneficiaries have "the right to be notified upon a breach of any of your unsecured health information."[9]

102. Similarly, in its "Trust Center[,]" Blue Shield represents it has a "laser focus on cybersecurity" to "continuously monitor and improve [Blue Shield's] governance, identify and access management, awareness and training, supply chain risks, and all other areas related to our people, processes, and technologies."[10] Blue Shield further represents it applies the National Association of Standards and Technology ("NIST"), which, among other things, recommends companies continuously monitor external service providers.[11]

Class Members

103. Plaintiff and Class Members are current and former Blue Shield members and beneficiaries, who provided and entrusted their PII and PHI to Defendants.

104. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

---

[6] *See* https://news.blueshieldca.com/cybersecurity-attack-on-vendors-files-may-have-impacted-blue-shield-of-california-member-data (last accessed Dec. 6, 2023).

[7] https://www.mesvision.com/cdn/NoticeOfSecurityIncident.pdf?v=8f5aeaedd3c1352e5ecaa798d5a3ee32 (last accessed Dec. 6, 2023).

[8] MESVision, *Privacy Policy*, https://www.mesvisionoptics.com/privacy#security6a9e9d84922c4313a283e1bb0a8f1adb (last accessed Dec. 6, 2023).

[9] MESVision, *HIPAA Notice*, https://www.mesvisionoptics.com/hipaa-notice (last accessed Dec. 6, 2023).

[10] Blue Shield, *Trust Center,* https://www.blueshieldca.com/en/home/about-blue-shield/privacy-and-security/trust-center (last accessed Dec. 6, 2023).

[11] NIST, *RMF Quick Start Guide* (Mar. 11, 2021), *available at* https://csrc.nist.gov/Projects/risk-management/about-rmf/monitor-step.

The Data Breach

105. On May 28 and 31, a ransomware gang exfiltrated Blue Shield members and beneficiaries' sensitive data through a vulnerability in MESVision's file transfer software(the "Vulnerability").

106. Researchers first discovered the Vulnerability on May 27, 2023. The Vulnerability was publicly announced to affected entities, including Defendants, on May 31, 2023. Impacted entities were instructed to modify their firewall rules until a patch could be applied, delete unauthorized files and user accounts, reset service account credentials, and apply the patch.[12] Affected entities, including Defendants, were further encouraged to adopt additional security best practices and look out for "indicators of compromise."[13]

107. On August 23, 2023, MESVision discovered that an unauthorized third party had accessed its information on a specific server.[14] The attack exposed the PII and PHI information of over 600,000 individuals, including Blue Shield members and beneficiaries.[15] For Blue Shield members and beneficiaries, the compromised PII and PHI includes, but is not limited to:

a. Full names;

b. dates of birth;

c. addresses;

d. subscriber ID numbers;

e. subscriber names;

f. subscriber date of birth;

g. subscriber Social Security numbers;

h. group ID numbers;

i. vision provider's name;

j. patient ID numbers;

---

[12] https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 (accessed Dec. 6, 2023).

[13] *Id.*

[14] https://news.blueshieldca.com/cybersecurity-attack-on-vendors-files-may-have-impacted-blue-shield-of-california-member-data (last accessed Dec. 6, 2023).

[15] https://oag.ca.gov/ecrime/databreach/reports/sb24-576536 (last accessed Dec. 6, 2023)

k. vision claims numbers;

l. vision related treatments and diagnosis information; and

m. vision related treatment cost information.[16]

108. In response, MESVision "took the server offline, launched an investigation into the incident, and engaged a cybersecurity firm."[17] And at an undisclosed date, between August 23, 2023, and November 10, 2023, MESVision determined the Data Breach occurred on May 28, and 31, and notified the FBI.[18] During that time, MESVision also took steps to improve its affected system.[19]

109. On September 1, 2023, Blue Shield received a notification from MESVision that MESVision had been the subject of the Data Breach and the Data Breach had impacted Blue Shield's members and beneficiaries.[20]

110. On November 14, 2023, 171 days after the Data Breach and 83 days after MESVision discovered the Data Breach, MESVision sent individual notices to members and beneficiaries impacted by the Data Breach.[21]

111. Similarly, on November 10, 2023, 167 days after the Data Breach and 70 days after Blue Shield learned of the Data Breach, Blue Shield sent individual notices to its members and beneficiaries impacted by the Data Breach.[22]

---

[16] https://news.blueshieldca.com/cybersecurity-attack-on-vendors-files-may-have-impacted-blue-shield-of-california-member-data (last accessed Dec. 6, 2023).

[17] https://oag.ca.gov/system/files/MES%20Individual%20Notice%20Template%2011.14.2023.pdf (last accessed Dec. 6, 2023).

[18] *Id.*; *see also Blue Shield Ltr. to Lew* (Nov. 10, 2023)

[19] *Id.*

[20] https://news.blueshieldca.com/cybersecurity-attack-on-vendors-files-may-have-impacted-blue-shield-of-california-member-data (last accessed Dec. 6, 2023).

[21] https://oag.ca.gov/system/files/MES%20Individual%20Notice%20Template%2011.14.2023.pdf (last accessed Dec. 6, 2023).

[22] https://oag.ca.gov/system/files/Blue%20Shield%20-%20Individual%20Notice%20Template%2011.17.2023%20%2812%20months%29.pdf (last accessed Dec. 6, 2023); *Blue Shield Ltr. to Lew* (Nov. 10, 2023).

Defendants failed to maintain adequate cybersecurity measures to prevent the breach

28. Defendants failed to reasonably and adequately protect the PII and PHI of Blue Shield's members and beneficiaries.

29. Prior to the Data Breach, both MESVision and Blue Shield had other vendors and sub-contractors who were the target of data breaches. For instance, DigiCert, a different MESVision vendor who provides file transfer services to MESVision, suffered a hack impacting its certificate systems, in 2020.[23] And, for Blue Shield, this Data Breach is the second it has experienced related to a sub-contractor this year. In March, Blue Shield disclosed that one of its providers had "suffered a security incident" in late January, which compromised its plan members' PII.[24] And Blue Shield has incurred at least eleven additional data breaches in the past ten years.[25]

30. Defendants were therefore on notice that their data was an attractive target to hackers, that their and their vendors' security measures were not reasonable or adequate, and that more stringent security measures were necessary to protect that data from being compromised.

31. Furthermore, according to industry sources, businesses rely on a set of vulnerability management metrics to help assess their cybersecurity health. Those metrics include, among other things: the mean time to detection ("MTTD")—that is, the average time it takes to "detect vulnerabilities or security flaws from the moment they first occur"; the mean time to remediate ("MTTR")—that is, the "average time taken to resolve and mitigate cybersecurity vulnerabilities from the time they are identified"; and the "average vulnerability age"—that is, the "average length of time that vulnerabilities exist within a computing

[23] https://www.theregister.com/2020/05/05/salt_vuln_digicert/ (last accessed Dec. 6, 2023).

[24] https://oag.ca.gov/system/files/EXPERIAN_J2010_BLUE_SHIELD_OF_CALIFORNIA_Fortra_Brightline_L01_SAS_0.pdf (last accessed Dec. 6, 2023).

[25] *See* *https://oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=blue+shield+of+california&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D=* (last accessed Dec. 6, 2023).

environment before being remediated." A healthy cybersecurity system minimizes both metrics.[26]

32. Defendants' response to the breach was deficient. While one survey found that the average MTTR for the Vulnerability was 7 days and the average vulnerability age was 56 days,[27] MESVision's MTTD to the Vulnerability was 88 days[28] and its MTTR was up to 79 days.[29] Similarly, Blue Shield did not discover the Data Breach until September 1, 2023, and may have taken up to November 10, 2023, to remediate the Vulnerability. Furthermore, the age of the Vulnerability for both Blue Shield and MESVision was up to 170 days—over three times longer than the vulnerability age for the average company affected by the same Vulnerability.

33. For further comparison, other entities impacted by the Vulnerability detected unusual activity and took action as early as May.[30] And many other entities began investigating whether their customers' data had been impacted immediately following the announcement of the Vulnerability as early as May 31.[31] Defendants' failure to timely detect and remediate the Data Breach demonstrates both companies lacked adequate security measures and cybersecurity infrastructure.

34. Defendants failed to implement and maintain reasonable security measures to prevent the Data Breach, such as auditing and monitoring the integrity of their vendors' data practices. Hackers gained access to Plaintiff and Class Members' PII and PHI through the

---

[26] https://heimdalsecurity.com/blog/vulnerability-management-metrics/ (last accessed Dec. 6, 2023).

[27] *Id.*

[28] The number of days between when the data was first exfiltrated on May 28, 2023, and when MESVision purportedly discovered the Data Breach, August 23, 2023.

[29] MESVision did not even discover the Data Breach until August 23, 2023, and while it took its effected server offline immediately, it may have taken MESVision up to November 10, 2023, to remediate the Vulnerability.

[30] *See, e.g.*, https://www.cms.gov/newsroom/press-releases/cms-responding-data-breach-contractor (last accessed Dec. 6, 2023) (Maximus).

[31] *See, e.g.*, https://www.mass.gov/doc/assigned-data-breach-number-29922-accelya-topco-limited/download (last accessed Dec. 7, 2023); https://www.jdsupra.com/legalnews/the-vitality-group-notifies-alfa-laval-3740655/ (last accessed Dec. 7, 2023); https://www.alleghenycounty.us/information-technology/notice-of-data-breach.aspx (last accessed Dec. 7, 2023).

software provided by MESVision's vendor. Had Defendants audited or monitored the integrity of the data practices of its vendors, they could have prevented the Breach.

35. Defendants also failed to timely detect and notify Blue Shield's members and beneficiaries of the Data Breach. Had Defendants detected and notified members and beneficiaries sooner, members and beneficiaries could have taken precautions to mitigate the impact. For instance, members and beneficiaries could have (1) purchased (or enhanced existing) identity protection, monitoring, and recovery services; (2) flagged asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchased or otherwise obtained credit reports; (4) placed or renewed fraud alerts on a quarterly basis; (5) intensively monitored their personal data; and (6) took other steps to protect themselves and attempt to avoid or recover from identity theft.

PII and PHI has concrete financial value

36. The PII and PHI taken from Defendants' systems is particularly sensitive. Medical and personally identifiable information is valuable to cybercriminals and has routinely been sold and traded on the dark web.

37. PHI and PII are inherently valuable, and it is becoming increasingly a frequent target of hackers. In 2022, a record 1,802 breaches occurred, resulting in approximately 442,143,312 sensitive records being exposed, a 48% increase from 2021.[32] Of the 1,802 recorded data breaches, 344 of them, or 19.1% were in the medical healthcare industry.[33] By comparison, in 2021, there were only 330 breaches, or 4.1% less breaches.[34] The 344 reported 2022 breaches exposed nearly 26 million sensitive records (26,259,933).[35]

38. Identity theft results in a significant negative financial impact on victims as well as severe distress.

---

[32] See 2022 Data Breach Annual Report (ITRC, Jan. 2023), *available at* https://notified.idtheftcenter.org/s/, at 8, 11.
[33] *Id.* at 11.
[34] *Id.*
[35] *Id.*

39. PHI and PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud. There is a robust black market in which criminals openly post stolen PHI and PII on multiple underground internet websites, commonly referred to as the dark web.

40. There is accordingly a market for Plaintiff and Class Members' PHI and PII. Sensitive healthcare data can sell for as much as $363 per record, according to the Infosec Institute. PHI is particularly valuable because criminals can use it to target victims with fraud and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

41. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, misdiagnosis or mistreatment can ensue. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[36]

42. Similarly, Social Security numbers are valuable to criminals. This information can be and has been sold and traded on the dark web black market. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

43. The detrimental consequences of Defendants' failure to keep its patients' and members' PHI and PII secure are long lasting and severe. Once PHI and PII is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might

[36] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ (last visited Dec. 6, 2023).

not show up for months or years.

44. Criminals often trade stolen PHI and PII on the "cyber black market" for years following a breach. Cybercriminals also can post stolen PHI and PII on the internet, thereby making the information publicly available without the knowledge or consent of the victim.

45. Defendants knew the importance of safeguarding the PHI and PII entrusted to them and the foreseeable adverse effects if its data security systems were breached. Those effects include the significant costs that would be imposed on affected patients as a result of a breach. Defendants failed to implement reasonable and adequate cybersecurity measures, leading to the Data Breach.

V. CLASS ACTION ALLEGATIONS

53. Plaintiff brings this consolidated action under Code of Civil Procedure section 382 on behalf of a Class of California Citizens who are Blue Shield members and beneficiaries whose PII and PHI was in MESVision's electronic information systems and was compromised as a result of the Data Breach. Excluded from the Class are Defendants and their officers, directors, and managerial employees. Also excluded is anyone employed by counsel for the parties in this action and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

54. Plaintiff reserves the right to modify, change, or expand the Class definition, including by proposing subclasses, based on discovery and further investigation.

55. Numerosity. While the exact number of Class Members is not known at this time, the estimated number of Class Members is over 600,000, making joinder of all members impractical. The identities of Class Members are readily ascertainable from information and records in the possession, custody, or control of Defendants, and notice of this action can be readily provided to the Class.

56. Typicality. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all Class Members, had his PII and PHI compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions of Defendants as

described herein. Accordingly, Plaintiff's claims arise from the same course of conduct that gives rise to the claims of all Class Members.

57. Adequacy of Representation. Plaintiff is a member of the proposed Class and will fairly and adequately represent and protect the other members' interests. Plaintiff's counsel are experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiff has no interests adverse to the interests of other Class Members.

58. Predominant Common Issues of Law and Fact. There is a well-defined community of interest in the common questions of law and fact that underlie Class Members' claims for relief. The questions of law and fact in this case that are common to Class Members predominate over questions affecting only individual Class Members. Among the questions of law and fact common to the Class are:

a. Whether Defendants had a duty to implement reasonable cybersecurity measures to protect Plaintiff and Class Members' sensitive personal information and to promptly alert them if such information was compromised;

b. Whether Defendants breached their duties by failing to take reasonable precautions to protect Plaintiff and Class Members' sensitive personal information;

c. Whether Defendants acted negligently by failing to implement reasonable data security practices and procedures;

d. Whether Defendants violated the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq.*;

e. Whether Defendants violated the California Confidentiality of Medical Information Act, Civ. Code § 56, *et seq.*;

f. Whether Defendants violated the California Customer Records Act, Civ. Code § 1798.80, *et seq.*;

g. Whether Defendants' failures to implement reasonable data security protocols and to timely notify Plaintiff and Class Members of the Data Breach violate the Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq.*; and

h. Whether Plaintiff and Class Members are entitled to statutory damages, actual damages, and/or injunctive and other relief in equity.

59. Superiority. A class action is superior to other alternatives for the fair and efficient adjudication of this controversy. Absent a class action, most members of the Class would find the cost of litigating their claims individually to be prohibitively high and would have no effective remedy. Class treatment will conserve judicial resources, avoid waste and the risk of inconsistent rulings, and promote efficient adjudication before a single Judge.

60. Injunctive and Declaratory Relief. Defendants have acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant injunctive and declaratory relief with respect to the Class as a whole.

FIRST CAUSE OF ACTION
Negligence
(Against MESVision and Blue Shield)

53. Plaintiff incorporates and realleges the foregoing allegations of fact.

54. Defendants collected and stored Plaintiff and Class Members' personal information, including member name, member date of birth, address, subscriber ID number, subscriber name, subscriber date of birth, subscriber Social Security number, group ID number, vision provider's name, patient ID number, vision claims number, vision related treatment and diagnosis information, and vision related treatment cost information.

55. Defendants owed Plaintiff and Class Members a duty of reasonable care to preserve and protect the confidentiality of their personal information that they collected. This duty included, among other obligations, maintaining and testing their and their vendors' security systems and computer networks, and taking other reasonable security measures to safeguard and adequately secure the personal information of Plaintiff and the Class from unauthorized access and use.

56. Defendants' duties also arise by operation of statute. The Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*, imposes a mandatory duty on MESVision and Blue Shield to implement and maintain reasonable security procedures and practices to safeguard and protect against the unauthorized disclosure of personal information.

57. Plaintiff and Class Members were the foreseeable victims of Defendants' inadequate and ineffectual cybersecurity. The natural and probable consequence of Defendants' failing to adequately secure their information networks was Plaintiff and Class Members' personal information being hacked.

58. Defendants knew or should have known that Plaintiff and Class Members' personal information was an attractive target for cyber thieves, particularly in light of data breaches experienced by themselves and their vendors, as well as other entities around the United States. Moreover, the harm to Plaintiff and Class Members from exposure of their highly confidential personal information was reasonably foreseeable to Defendants.

59. Defendants had the ability to sufficiently guard against data breaches by monitoring and testing their vendors' systems and implementing adequate measures to protect their systems, such as using attack surface intelligence software. Moreover, Defendants had the ability to mitigate the harm from the Breach by monitoring their vendors' systems for unusual activity, investigating their software when the Vulnerability was announced, and promptly installing the patch.

60. Defendants breached their duty to exercise reasonable care in protecting Plaintiff and Class Members' personal information by failing to implement and maintain adequate security measures to safeguard Plaintiff and Class Members' personal information, failing to monitor their systems to identify suspicious activity, and allowing unauthorized access to, and exfiltration of, Plaintiff and Class Members' confidential personal information.

61. Defendants also owed a duty to timely disclose to Plaintiff and Class Members that their personal information had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that Plaintiff and Class Members could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) place or renew fraud alerts on a quarterly basis; (5) intensively monitor loan data and public

records; and (6) take other steps to protect themselves and attempt to avoid or recover from identity theft.

62. Defendants breached their duty to timely disclose the Data Breach to Plaintiff and Class Members. After learning of the Data Breach, Defendants unreasonably delayed in notifying Plaintiff and Class Members of the Data Breach. This unreasonable delay caused foreseeable harm to Plaintiff and Class Members by preventing them from taking timely self-protection measures in response to the Data Breach.

63. There is a close connection between Defendants' failure to employ reasonable security protections for its employees' personal information and the injuries suffered by Plaintiff and Class Members. When individuals' sensitive personal information is stolen, they face a heightened risk of identity theft and may need to: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries and charges; (5) place and renew credit fraud alerts on a quarterly basis; (6) contest fraudulent charges and other forms of identity theft; (7) repair damage to credit and financial accounts; and (8) take other steps to protect themselves and attempt to avoid or recover from identity theft and fraud.

64. Defendants were in a special relationship with Plaintiff and Class Members with respect to the hacked information because the end and aim of Defendants' data security measures was to benefit Plaintiff and Class Members by ensuring that their personal information would remain protected and secure. Only Defendants were in a position to ensure that their systems were sufficiently secure to protect Plaintiff and Class Members' personal and medical information. The harm to Plaintiff and Class Members from its exposure was highly foreseeable to Defendants.

65. The policy of preventing future harm disfavors application of the economic loss rule, particularly given the sensitivity of the private information entrusted to Defendants. A high

degree of opprobrium attaches to Defendants' failure to secure Plaintiff and Class Members' personal and extremely confidential facts. Defendants had an independent duty in tort to protect this information and thereby avoid reasonably foreseeable harm to Plaintiff and Class Members.

66. As a result of Defendants' negligence, Plaintiff and Class Members have suffered damages that have included or may, in the future, include, without limitation: (1) loss of the opportunity to control how their personal information is used; (2) diminution in the value and use of their personal information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (3) the compromise and theft of their personal information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (5) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (6) unauthorized use of compromised personal information to open new financial and other accounts; (7) continued risk to their personal information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in its possession; and (8) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

SECOND CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018
Civ. Code § 1798.100, *et seq.* ("CCPA")
(Against MESVision and Blue Shield)

67. Plaintiff incorporates and realleges the foregoing allegations of fact.

68. Section 1798.150(a)(1) of the CCP provides, "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined by [Civil Code section 1798.81.5(d)(1)(A)] . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal

information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

69. Plaintiff is a consumer and California resident as defined by Civil Code section 1798.140(i).

70. Defendant MESVision is a "business" as defined by Civil Code section 1798.140(d)(1) because it is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California . . . [and] alone or in combination, annually buys, sells or shares the personal information of 100,000 or more consumers or households."

71. MESVision collects personal information from, among other sources, consumers who request information from it, consumers who use its services, including users of its mobile applications, and consumers who submit customer support requests.

72. MESVision annually buys, sells, or shares, alone or in combination, the personal information of 100,000 or more consumers or households.

73. Blue Shield is a "business" as defined by Civil Code section 1798.140(d)(2) because it shares common branding and controls entities that are "organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the state of California."

74. Both Blue Shield and Blue Shield of California Life & Health Insurance Company do business as "Blue Shield of California" and share a website.[37]

[37] https://www.blueshieldca.com/en/home (last accessed Dec. 13, 2023).

75. Blue Shield holds one hundred percent ownership of Blue Shield of California Life & Health Insurance Company.[38]

76. Blue Shield of California Life & Health Insurance Company is a "business" as defined by Civil Code section 1798.140(d)(1) because it is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California . . . [and] alone or in combination, annually buys, sells or shares the personal information of 100,000 or more consumers or households."

77. Blue Shield of California Life & Health Insurance Company collects personal information from, among other sources, consumers who request information from it, consumers who use its services, including users of its mobile applications, and consumers who submit customer support requests.

78. Blue Shield of California Life & Health Insurance Company, "[a]lone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households" and has an annual gross revenue in excess of $25 million.[39]

79. Plaintiff and Class Members' personal information, as defined by Civil Code section 1798.140(v)(1),was subject to unauthorized access and exfiltration, theft or disclosure. The Data Breach described herein exposed, without limitation, member name, member date of birth, address, subscriber ID number, subscriber name, subscriber date of birth, subscriber Social Security number, group ID number, vision provider's name, patient ID number, vision claims

[38] *Blue Shield of California Life & Health Insurance Company – as of 12-31-20*, https://www.insurance.ca.gov/0250-insurers/0300-insurers/0400-reports-examination/ (last accessed Dec. 13, 2023).

[39] https://www.blueshieldca.com/en/home/about-blue-shield/corporate-information/financials (last accessed Dec. 13, 2023).

number, vision related treatment and diagnosis information, and vision related treatment cost information.[40]

80. MESVision and Blue Shield maintained Plaintiff and Class Members' PII in a form that allowed criminals to access it.

81. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices for protecting the exposed information given its nature. Defendants failed to monitor its systems to identify suspicious activity and allowed unauthorized access to Plaintiff and Class Members' PII.

82. Consistent with Civil Code section 1798.150, Plaintiff provided written notice to Defendants identifying the CCPA provisions that Defendants violated. If Defendants are unable to cure or does not cure the violation within 30 days, Plaintiff will amend this complaint to pursue actual or statutory damages, as permitted by Civil Code section 1798.150(b).

83. Plaintiff presently seeks injunctive and declaratory relief, and any other relief as deemed appropriate by the Court for Defendants' CCPA violations.

THIRD CAUSE OF ACTION
Violation of the California Confidentiality of Medical Information Act
Civ. Code § 56, *et seq.* ("CMIA")
(Against MESVision and Blue Shield)

84. Plaintiff incorporates and realleges the foregoing allegations of fact.

85. Each Defendant is a "provider of health care" as defined in Civil Code section 56.06. Each Defendant is organized in part for the purpose of maintaining medical information to make it available to an individual or provider of health care for purposes of information management, diagnosis, or treatment. Blue Shield is a California-based mutual benefit corporation and health plan provider with over 4.8 million members.[41] MESVision is a

[40] *See* https://news.blueshieldca.com/cybersecurity-attack-on-vendors-files-may-have-impacted-blue-shield-of-california-member-data (last accessed Dec. 6, 2023).

[41] https://news.blueshieldca.com/about#:~:text=Blue%20Shield%20of%20California%20is,%2424%20billion%20in%20annual%20revenue. (last accessed Dec. 6, 2023).

California-based vision benefit program provider and administrator who provides administration services to all Blue Shield vision benefit plans.[42]

86. Plaintiff and Class Members are "patients" within the meaning of Civil Code section 50.05(k), and are "endanger[ed]" within the meaning of Civil Code section 56.05(e) because Plaintiff and Class Members reasonably fear that disclosure of their medical information could subject them to abuse, extortion, or other harassment or harm.

87. Plaintiff and Class Members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code section 56.05(j), created, maintained, preserved, stored, abandoned, destroyed or disposed of on or through Defendants' computer networks at the time of the Data Breach.

88. Defendants violated Civil Code section 56.101 by failing to maintain and preserve the confidentiality of Plaintiff and Class Members' medical information.

89. In violation of Civil Code section 56.101(a), Defendants negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff and Class Members' medical information in a manner that failed to preserve the security of that information and breached its confidentiality. As a result, Plaintiff and Class Members' confidential information and records were negligently released to hackers in the Data Breach.

90. Medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as defined by Civil Code section 56.101(c).

91. That the information taken in the breach was accessed by unauthorized individuals is evidenced by the fact that the personal information is likely in the possession of ransomware hackers. The information was necessarily viewed to be used in this manner.

92. In violation of Civil Code section 56.101(b)(1)(A), Defendants' electronic health record systems or electronic medical record systems failed to protect and preserve the integrity of electronic medical information.

---

[42] https://www.blueshieldca.com/bsca/bsc/wcm/connect/member/member_content_en/content%20root/ifp/plan_resources/your_vision_plan#:~:text=Blue%20Shield%20vision%20plans%20are,and%20are%20administered%20by%20MESVision. (last accessed Dec. 6, 2023).

93. Defendants also violated Civil Code section 56.36(b) by negligently releasing Plaintiff and Class Members' confidential information in the Data Breach.

94. Defendants' wrongful conduct, actions, inaction, omissions, and want of ordinary care violate the CMIA and directly and proximately caused the Data Breach. Plaintiff and Class Members consequently have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their medical information; (2) loss of the opportunity to control how their medical information is used; (3) diminution in the value and use of their medical information entrusted to Defendants with the understanding that Defendants would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their medical information; (5) continued undue risk to their medical information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their medical information being stolen in the Data Breach.

95. Plaintiff and Class Members were injured and have suffered damages, as described above, from Defendants' negligent release of their medical information in violation of Civil Code sections 56.36, and 56.101, and accordingly are entitled to relief under Civil Code 56.36, including actual damages, nominal statutory damages of $1,000, injunctive relief, and attorney fees, expenses and costs.

FOURTH CAUSE OF ACTION
Violation of the California Customer Records Act, Civ. Code § 1798.80, *et seq.* ("CCRA")
(Against MESVision and Blue Shield)

96. Plaintiff incorporates and realleges the foregoing allegations of fact.

97. Plaintiff and Class Members are "customers" within the meaning of Civil Code section 1798.80(c), as they provided personal information to MESVision and Blue Shield for the purpose of obtaining services.

98. MESVision and Blue Shield are "business[es]" within the meaning of Civil Code section 1798.80(a).

99. The CCRA provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person . . . in the most expedient time possible and without unreasonable delay[.]" Civ. Code § 1798.82.

100. The Data Breach was a breach of security within the meaning of section 1798.82. PII stolen in the Data Breach, such as member name, member date of birth, address, subscriber ID number, subscriber name, subscriber date of birth, subscriber Social Security number, group ID number, vision provider's name, patient ID number, vision claims number, vision related treatment and diagnosis information, and vision related treatment cost information, as well as other information, constitutes "personal information" within the meaning of section 1798.80(e).

101. In violation of the CCRA, MESVision and Blue Shield unreasonably delayed in notifying Plaintiff and Class Members of the Data Breach. MESVision was aware of the Data Breach by no later than August 23, 2023, but it did not announce the Data Breach until November 14, 2023. Similarly, Blue Shield was aware of the Data Breach by no later than September 2, 2023, but it did not announce the Data Breach until November 10, 2023. There were no legitimate law enforcement needs justifying these delays. Nor were the delays necessary to determine the scope of the breach and restore the reasonable integrity of MESVision or Blue Shield's electronic data systems.

102. Timely disclosure was necessary so that Plaintiff and Class Members could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) place or renew fraud alerts on a quarterly basis; (5) intensively monitor loan data and public records; and (6) take other steps to protect themselves and attempt to avoid or recover from identity theft.

103. As a result of MESVision and Blue Shield's unreasonable delay of at least two months in notifying Plaintiff and Class Members of the Data Breach, they were deprived of an opportunity to take timely and appropriate self-protective measures, such as requesting a credit freeze. In addition, as a result of the delay, Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their personal information; (2) loss of the opportunity to control how their personal information is used; (3) diminution in the value and use of their personal information entrusted to Defendants with the understanding that Defendants would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their personal information; (5) continued undue risk to their personal information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

104. Therefore, on behalf of the Class, Plaintiff seeks actual damages under Civil Code section 1798.84(b), injunctive and declaratory relief, and any other relief deemed appropriate by the Court.

FIFTH CAUSE OF ACTION
Violation of the Unfair Competition Law,
Bus. & Prof. Code § 17200 *et seq.* ("UCL")
(Against MESVision and Blue Shield)

105. Plaintiff incorporates and realleges the foregoing allegations of fact.

106. The UCL proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

107. MESVision's conduct is unlawful, in violation of the UCL, because it violates the CMIA, CCPA, and the CCRA. Blue Shield's conduct is unlawful, in violation of the UCL, because it violates the CMIA and CCRA.

108. Defendants' conduct is substantially unfair, predatory, and contrary to California's and the nation's legislatively declared public policy in favor of protecting the privacy and

security of personal and confidential information. *See* S. Rep. No. 100-500 at 7-8 (1988) (finding that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems . . . create[s] privacy interests that directly affect the ability of people to express their opinions, to join in association with others, and to enjoy the freedom and independence that the Constitution was established to safeguard."); California Bill Analysis, A.B. 375 Assem. (June 27, 2021) (noting that "[t]unregulated and unauthorized disclosure of personal information and the resulting loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to the destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.").

109. MESVision and Blue Shield's conduct also is unfair and deceptive in violation of the UCL. Defendants' unfair business acts and practices include:

a. failing to adequately secure the personal information of Plaintiff and Class Members from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about Plaintiff and Class Members in a manner highly offensive to a reasonable person;

c. enabling the disclosure of personal and sensitive facts about Plaintiff and Class Members without their informed, voluntary, affirmative, and clear consent; and

d. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiff and Class Members from taking timely self-protection measures.

110. The gravity of harm resulting from MESVision and Blue Shield's unfair conduct outweighs any potential utility. The failure to adequately safeguard personal, sensitive information harms the public at large and is part of a common and uniform course of wrongful conduct.

111. The harm from MESVision and Blue Shield's conduct was not reasonably avoidable by consumers. The individuals affected by the Data Breach—Blue Shield's members and beneficiaries—were required to provide their PII as part of their relationship with MESVision and Blue Shield. Plaintiff and Class Members did not know of, and had no

reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures. Nor did any member of the Class have any means of preventing the Data Breach.

112. There were reasonably available alternatives that would have furthered MESVision and Blue Shield's business interests of electronically transferring their customers' information while protecting PII, such as discontinuing use of insecure file transfer applications and ensuring best practices in cybersecurity defense.

113. MESVision and Blue Shield's omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of Plaintiff and Class Members' personal information. A reasonable person would regard MESVision and Blue Shield's derelict data security and the Data Breach as important, material facts. MESVision and Blue Shield could and should have timely disclosed these facts.

114. As a direct and proximate result of MESVision and Blue Shield's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff lost money or property because their sensitive personal information experienced a diminution of value and because they devoted additional time—which they otherwise would or could have devoted to pecuniary gain—to monitoring their credit reports and financial accounts for fraudulent activity.

115. Plaintiff and Class Members therefore seek all monetary and non-monetary relief permitted by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs under Code of Civil Procedure section 1021.5.

SIXTH CAUSE OF ACTION
Invasion of Privacy
(Against MESVision and Blue Shield)

116. Plaintiff incorporates and realleges the foregoing allegations of fact.

117. Defendants wrongfully intruded upon Plaintiff and Class Members' seclusion in violation of California law. Plaintiff and Class Members reasonably expected that the personal information they entrusted to Defendants, such as their name, date of birth, address, subscriber ID number, subscriber name, subscriber date of birth, subscriber Social Security number, group

ID number, vision provider's name, patient ID number, vision claims number, vision related treatment and diagnosis information, and vision related treatment cost information.

118. Defendants unlawfully invaded Plaintiff and Class Members' privacy rights by:

a. failing to adequately secure their personal information from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

119. A reasonable person would find it highly offensive that Defendants, having received, collected, and stored Plaintiff and Class Members' birthdates, Social Security numbers, and other personal details, failed to protect that information from unauthorized disclosure to third parties.

120. In failing to adequately protect Plaintiff and Class Members' personal information, Defendants acted knowingly and in reckless disregard of their privacy rights. Defendants also knew or should have known that their ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiff's position.

121. Defendants' unlawful invasions of privacy damaged Plaintiff and Class Members. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff and Class Members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for an order:

A. Certifying this case as a class action, appointing Plaintiff as a Class representatives, and appointing Plaintiff's counsel to represent the Class;

B. Entering judgment for Plaintiff and the Class;

C. Awarding Plaintiff and Class Members monetary relief, including nominal and statutory damages;

D. Ordering appropriate injunctive or other equitable relief;

E. Awarding pre- and post-judgment interest as prescribed by law;

F. Awarding reasonable attorneys' fees and costs as permitted by law; and

G. Granting such further and other relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: December 13, 2023

Respectfully submitted,

By: */s/ Simon S. Grille*

Adam E. Polk (State Bar No. 273000)
Simon Grille (State Bar No. 294914)
Jordan N. Isern (State Bar No. 343159)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
sgrille@girardsharp.com
apolk@girardsharp.com
jisern@girardsharp.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org
