Exhibit A1

Cristina Perez Hesano (#027023)
cperez@perezlawgroup.com
PEREZ LAW GROUP, PLLC
7508 N. 59th Avenue
Glendale, AZ 85301
Telephone: 602.730.7100
Fax: 623.235.6173

Gary M. Klinger *(pro hac vice)*
gklinger@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878

Attorneys for Plaintiff and the proposed Class

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Linda Hulewat; Karen Foti Williams; Ralph Gallegos; Michael Martinez; Lynnae Anderson; Candia Franklin; Marie Therese Montoya; Charles Peterson; Robert Kirk; Marilyn Zajacka; Lynda Israel; Latricia Pelt; Barry Pelt; Ken Waters; Brenda Moreno-Decerra; Robert Ahrensdorf; and David Yeager; individually, and all others similarly situated,

Plaintiffs,

v.

Medical Management Resource Group, L.L.C.; Barnet Dulaney Perkins Eye Center, PC; Marc Ellman, M.D., P.A. d/b/a Southwest Eye Institute; Southwestern Eye Center, Ltd.; Eye Associates of Nevada d/b/a Wellish Vision Institute,

Defendants.

Case No. 2:24-cv-00377-DJH

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Linda Hulewat, Karen Foti Williams, Ralph Gallegos, Michael Martinez, Lynnae Anderson, Candia Franklin, Marie Therese Montoya, Charles Peterson, Robert Kirk, Marilyn Zajacka, Lynda Israel, Latricia Pelt, Barry Pelt, Ken Waters, Brenda Moreno-Decerra, Robert Ahrensdorf, and David Yeager ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint against Defendants Barnet Dulaney Perkins Eye Center, PC ("Barnet"), Marc Ellman, M.D., P.A., d/b/a Southwest Eye Institute ("SWEI"), Southwestern Eye Center, Ltd. ("SWEC"), and Eye Associates of Nevada d/b/a Wellish Vision Institute ("Wellish") (collectively, "Ophthalmologist Defendants"), and Defendant Medical Management Resource Group LLC d/b/a American Vision Partners ("American Vision" and, together with Ophthalmologist Defendants, "Defendants"). Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendants' failure to protect highly sensitive data.

2. American Vision "is one of the nation's largest and fastest-growing eye care physician services organizations" with "more than 180 nationally recognized doctors and 120 locations" across the country.[1] And American Vision advertises that "[w]e partner with the

[1] *Dr. Kent Wellish Successfully Implants First Bausch + Lomb Toric Aspire "Range of Vision" IOL in Las Vegas*, AMERICAN VISION PARTNERS (March 7, 2024) https://americanvisionpartners.com/press/wellish-first-bausch-lomb-toric-aspire-iol-las-vegas/.

most respected ophthalmology practices in the country and share a best-in-class management system, infrastructure, and technology to provide the highest-quality patient care."[2]

3. As such, American Vision partners with Ophthalmologist Defendants. Under this partnership, Ophthalmologist Defendants share patients' and employees' highly sensitive personally identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—and other data with American Vision. In turn, American Vision stores a litany of PII/PHI about Ophthalmologist Defendants' current and former employees and patients.

4. By collecting and storing the PII/PHI of Ophthalmologist Defendants' current and former employees and patients that is routinely targeted by cybercriminals, American Vision in turn had a resulting duty to safeguard such information from unauthorized access. But despite this duty, however, American Vision lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach and exfiltrated the PII/PHI stored therein (the "Data Breach").

5. It is unknown for precisely how long the cybercriminals had access to American Vision's network before the Data Breach was discovered. American Vision had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to current and former employees' and patients' PII/PHI.

6. The Data Breach occurred because American Vision failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols

[2] *Id.*

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

to protect the Class's PII/PHI. In short, American Vision's failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

7. Just as blameworthy are the Ophthalmologist Defendants. Each Ophthalmologist Defendant is responsible for the Data Breach by failing to exercise appropriate managerial control over American Vision's data security and the data they share with American Vision, which was its right as partners in the partnership, when they knew American Vision was storing PII/PHI and when they knew or should have known American Vision was unequipped to protect this information. Ophthalmologist Defendants also failed to exercise appropriate discretion in selecting their business associates with whom they chose to partner and share Plaintiffs' and Class Members' PII/PHI.

8. Plaintiffs are Data Breach victims. They bring this class action on behalf of themselves, and all others harmed by Defendants' misconduct.

9. As a result of Defendants' failure to protect the sensitive information they were entrusted to safeguard, Plaintiffs and Class members did not receive the benefit of their bargain with Defendants and face a significant risk of medical-related identity theft and fraud, financial fraud, and/or other identity-related fraud now and into the indefinite future.

10. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this Data Breach, Defendants' current and former employees' and patients' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

11. Plaintiff Linda Hulewat is a natural person and citizen of Nevada.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

12. Plaintiff Karen Foti Williams is a natural person and citizen of Arizona.

13. Plaintiff Ralph Gallegos is a natural person and citizen of Texas.

14. Plaintiff Michael Martinez is a natural person and citizen of Arizona.

15. Plaintiff Lynnae Anderson is a natural person and citizen of Arizona.

16. Plaintiff Candia Franklin is a natural person and citizen of Arizona.

17. Plaintiff Marie Therese Montoya is a natural person and citizen of Arizona.

18. Plaintiff Charles Peterson is a natural person and citizen of Arizona.

19. Plaintiff Robert Kirk is a natural person and citizen of Arizona.

20. Plaintiff Marilyn Zajacka is a natural person and citizen of Arizona.

21. Plaintiff Lynda Israel is a natural person and citizen of Nevada.

22. Plaintiff Latricia Pelt is a natural person and citizen of Michigan.

23. Plaintiff Barry Pelt is a natural person and citizen of Michigan.

24. Plaintiff Ken Waters is a natural person and citizen of Arizona.

25. Plaintiff Brenda Moreno-Decerra is a natural person and citizen of Arizona.

26. Plaintiff Robert Ahrensdorf is a natural person and citizen of Arizona.

27. Plaintiff David Yeager is a natural person and citizen of Arizona.

28. Defendant Medical Management Resource Group LLC, d/b/a American Vision Partners, is a limited liability company formed under the laws of Arizona and with its principal place of business at 63 S Rockford Drive, Suite 220, Tempe, Arizona 85281.

29. Defendant Barnet Dulaney Perkins Eye Center, PC is a professional corporation formed under the laws of Arizona and with its principal place of business at 4800 N 22nd St, Phoenix, Arizona 85016.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

30. Defendant Eye Associates of Nevada d/b/a Wellish Vision Institute is a professional corporation formed under the laws of Nevada and with its principal place of business at 701 S. Carson St., Suite 200, Carson City, Nevada 89701.

31. Defendant Southwestern Eye Center, Ltd. is a limited company formed under the laws of Arizona and with its principal place of business at 2610 E. University Dr., Mesa, Arizona 85213.

32. Defendant Marc Ellman, M.D., P.A., d/b/a Southwest Eye Institute is a profit professional association formed under the laws of Texas and with its principal place of business at 1400 Common Dr., El Paso, Texas 79936.

JURISDICTION AND VENUE

33. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. §§ 1332(d)(2), (d)(10).[3] The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom, including Plaintiffs, have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[3] When subject matter jurisdiction is established under the Class Action Fairness Act, "an LLC's citizenship is based on its principal place of business and laws of incorporation." *Hernandez v. Pure Health Rsch. LLC*, No. 23-cv-00971, 2023 U.S. Dist. LEXIS 191909, at *7 (S.D. Cal. Oct. 25, 2023) (applying § 1332(d)(10) of CAFA) (citing *Jack v. Ring LLC*, 553 F. Supp. 3d 711, 715 (N.D. Cal. 2021)); *see also Abrego v. Dow Chem. Co.*, 443 F.3d 676, 684 (9th Cir. 2006) (noting that § 1332(d)(10) of CAFA provides a different rule for unincorporated associations). Here, Defendant is an LLC formed under the laws of Arizona and with its principal place of business in Arizona. Thus, for the purposes of establishing minimal diversity, Defendant is a citizen of Arizona.

34. This Court also has personal jurisdiction over Defendants because they are headquartered in Arizona, regularly conduct business in Arizona, and have sufficient minimum contacts in Arizona.

a. Medical Management Resource Group LLC, is formed under the laws of Arizona, has its principal place of business in Arizona, and has sufficient minimum contacts in Arizona.

b. Barnet Dulaney Perkins Eye Center, PC is formed under the laws of Arizona, has its principal place of business in Arizona, and has sufficient minimum contacts in Arizona.

c. Eye Associates of Nevada d/b/a Wellish Vision Institute has sufficient minimum contacts in Arizona through its partnership with American Vision Partners. And upon information and belief, Wellish Vision Institute's patients include Arizona citizens (e.g., its website advertises that it accepts insurance from "BCBS Arizona").[4]

d. Southwestern Eye Center, Ltd. is formed under the laws of Arizona, has its principal place of business in Arizona, and has sufficient minimum contacts in Arizona.

e. Marc Ellman, M.D., P.A., d/b/a Southwest Eye Institute has sufficient minimum contacts in Arizona through its partnership with American Vision Partners.

[4] *Insurances Accepted by Our Eye Center*, WELLISH VISION INSTITUTE, https://www.wellishvision.com/your-visit/accepted-insurances/ (last visited July 26, 2024).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

35. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because this is the judicial district in which a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred

BACKGROUND

Defendants' Privacy Practices

36. American Vision "is one of the nation's largest and fastest-growing eye care physician services organizations" with "more than 180 nationally recognized doctors and 120 locations" across the country.[5] It advertises that "[w]e partner with the most respected ophthalmology practices in the country and share a best-in-class management system, infrastructure, and technology to provide the highest-quality patient care."[6]

37. As part of its business, American Vision collects and stores PII/PHI from millions of employees and patients of the Ophthalmologist Defendants. As a result, patients and employees do not voluntarily provide their PII/PHI to American Vision, but rather, Ophthalmologist Defendants unilaterally provide it to American Vision.

38. In collecting and maintaining the PII/PHI, Defendants agreed they would safeguard the data in accordance with their internal policies, state law, and federal law.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[5] *Dr. Kent Wellish Successfully Implants First Bausch + Lomb Toric Aspire "Range of Vision" IOL in Las Vegas*, AMERICAN VISION PARTNERS (March 7, 2024) https://americanvisionpartners.com/press/wellish-first-bausch-lomb-toric-aspire-iol-las-vegas/.

[6] *Id*.

39. Given the amount and sensitive nature of the data they collect, disclose, and store, Defendants maintain "Privacy Practices," describing their commitments and obligations for the use and disclosure of confidential information.

40. Recently, American Vision removed a "HIPAA Notice of Privacy Practices" dated October 1, 2020, from its website.[7] However, the policy is readily accessible via the "Internet Archive." And via the policy, American Vision promised as follows:

a. "This notice describes how medical information about you may be used and disclosed and how you can get access to this information."[8]

b. "Your medical information is personal. American Vision Partners and all of their affiliates ('AVP') and its employees are dedicated to maintaining the privacy of your personal health information ('PHI'), as required by applicable federal and state laws."[9]

c. "We are required to follow the privacy practices described[.]"[10]

d. "Psychotherapy Notes. We must receive your written authorization to disclose psychotherapy notes[.]"[11]

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[7] *HIPAA Notice of Privacy Practices*, AMERICAN VISION PARTNERS (Oct. 1, 2020) https://americanvisionpartners.com/notices/privacy-policy/ [https://web.archive.org/web/20230208043537/https://americanvisionpartners.com/notices/privacy-policy/].
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*

e. "Right to Notice of Breach. You have the right to be notified if we or one of our Business Associates becomes aware of a breach of your unsecured PHI."[12]

f. "We support your right to the privacy of your PHI."[13]

g. "Not Otherwise Permitted. In any other situation not described . . . we may not disclose your PHI without your written authorization."[14]

41. Notably, Ophthalmologist Defendants have copied and incorporated American Vision's "HIPAA Notice of Privacy Practices" onto their own ***patient-facing*** websites. Critically, the substantive language in these policies is ***identical***. The affiliates with the copied "HIPAA Notice of Privacy Practices" include Barnet,[15] Wellish,[16] and SWEI.[17]

42. In these policies, the affiliates direct their patients to "[p]lease direct any of your questions or complaints" to American Visions' (1) physical address, (2) phone number, (3)

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *HIPAA Notice of Privacy Practices*, BARNET DULANEY PERKINS EYE CENTER (Oct. 1, 2020) https://www.goodeyes.com/privacy-policy/.
[16] *HIPAA Notice of Privacy Practices*, WELLISH VISION INSTITUTE (Oct. 1, 2020) https://www.wellishvision.com/privacy-policy/.
[17] *HIPAA Notice of Privacy Practices*, SOUTHWESTERN EYE CENTER (Oct. 1, 2020) https://www.sweye.com/privacy-policy/.

email address, and (4) general counsel Rose Willis.[18] Ms. Willis is the General Counsel of American Vision.[19]

43. SWEC includes additional promises. For example, SWEC maintains a "Notice to Patients – Policy for Medical Record Retention, Maintenance and Destruction" stating that:

a. "Records shall be retained in accordance with all applicable laws, regulations and this policy."[20]

b. "Records that have satisfied their required period of retention and are no longer required shall be destroyed in an appropriate manner consistent with this policy."[21]

c. "All records will be maintained and retained in accordance with federal and state laws and regulations."[22]

d. "Offsite storage facilities are utilized to store records in a secure location that protects them from . . . [m]an-made hazards, such as theft, accidental

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[18] *See e.g., HIPAA Notice of Privacy Practices*, ABRAMS EYE INSTITUTE (Oct. 1, 2020) https://www.abramseyeinstitute.com/privacy-policy/; *Rose Willis*, AMERICAN VISION PARTNERS, https://americanvisionpartners.com/about/our-leadership/rose-willis/ (last visited July 19, 2024).

[19] *Data Breach Notifications*, MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/1c20fc77-1b3a-44a9-81e0-362f8bed0912.shtml (last visited July 24, 2024).

[20] *HIPAA Notice of Privacy Practices*, SOUTHWESTERN EYE CENTER (Oct. 1, 2020) https://www.sweye.com/wp-content/uploads/2020/09/SEC-NM-HIPAA-Notice-of-Privacy-Practices1.pdf.

[21] *Id.*

[22] *Id.*

loss, and sabotage . . . [and] [u]nauthorized use, disclosure and destruction."[23]

e. "Records are to be stored in secure cabinets or rooms that protect them from the following . . . [m]an-made hazards, such as theft, accidental loss, and sabotage . . . [u]nauthorized use, disclosure and destruction."[24]

f. "Records will be secured at the end of the day."[25]

g. Access will be limited to those working directly with the patient and/or coordinating the patient's care."[26]

h. "The company will select appropriate media and systems for storing records[.]"[27]

i. "Medical records stored on electronic media may be stored on or off- site but must be maintained under the same confidentiality standards and safe storage constraints as paper medical record charts."[28]

44. Also, SWEI provides a "Notice of Privacy Practices" stating that:

a. "This notice describes how medical information about you may be used and disclosed and how you can get access to this information."[29]

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Notice Of Privacy Practices*, SOUTHWEST EYE INSTITUTE, https://southwesteye.com/notice-of-privacy-practices (last visited July 18, 2024).

b. "We are required by law to maintain the privacy of your protected health information (PHI)."[30]

c. "This notice applies to all records of the health care and services you received[.]"[31]

d. "We are required by law to: make sure that your PHI is kept private . . . [and] train our personnel concerning privacy and confidentiality; and mitigate (lessen the harm of) any breach of privacy/confidentiality."[32]

e. "[A]ll of the ways we are permitted to use and disclose information fall within the categories [listed]."[33]

f. "Uses or disclosures of your PHI for other purposes or activities not listed above will be made only with your written authorization (permission)."[34]

45. Given Defendants' avowed experience handling highly sensitive PHI, Defendants understood the need to protect PII/PHI and prioritize data security for not only themselves but for their partners with whom they share PII/PHI.

American Vision's Data Breach

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*

46. On November 14, 2023, American Vision's systems were compromised in the Data Breach.[35]

47. American Vision acknowledged that not only did it "detect unauthorized activity" but also that "the unauthorized party ***obtained*** personal information associated with patients[.]"[36]

48. Because of the Data Breach, at least the following types of PII/PHI were compromised:

a. names;

b. Social Security numbers ("SSNs");

c. driver's license numbers;

d. passport numbers;

e. state ID card information;

f. government-issued ID numbers;

g. addresses;

h. contact information;

i. dates of birth;

j. financial account information;

k. bank account numbers;

l. credit card numbers;

[35] *Data Breach Notifications*, MAINE ATTY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/1c20fc77-1b3a-44a9-81e0-362f8bed0912.shtml (last visited July 18, 2024).

[36] *Id*. (emphasis added).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

m. debit card numbers;

n. health insurance information; and

o. medical information (including services received, clinical records, and medications).[37]

49. In total, at least 2,350,236 persons had their PII/PHI exfiltrated from American Visions' systems as part of the Data Breach.[38] Upon information and belief, these individuals consist of current and former employees and patients of the Ophthalmologist Defendants.[39]

50. And yet, American Vision waited until February 15, 2024, before it began notifying the class—a full 93 days after the Data Breach was discovered.[40]

51. By keeping affected individuals in the dark about the key details surrounding the Data Breach, Defendants prevented affected individuals from taking meaningful, proactive, and targeted mitigation measures that could help protect them against severe harm.

52. And when American Vision did notify Plaintiffs and the Class of the Data Breach, it acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class to:

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[37] *Data Security Breach Reports*, ATTY GEN TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited July 18, 2024); *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/1c20fc77-1b3a-44a9-81e0-362f8bed0912.shtml (last visited July 18, 2024).

[38] *Cases Currently Under Investigation*, US DEPT HEALTH & HUMAN SERVS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited July 17, 2024).

[39] *Id.*

[40] *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/1c20fc77-1b3a-44a9-81e0-362f8bed0912.shtml (last visited July 18, 2024).

a. "remain vigilant against incidents of identity theft and fraud by monitoring your free credit reports and reviewing your account statements;"

b. "obtain a police report and request a security freeze;"

c. "receive your credit report [and] review it carefully;"

d. "obtain information from [your] Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online[.]"[41]

53. It is well known that use of stolen credentials has long been the most popular and effective method of gaining authorized access to a company's internal networks and that companies should activate defenses to prevent such attacks.

54. According to the Federal Bureau of Investigation ("FBI"), phishing schemes designed to induce individuals to reveal personal information were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[42] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[43]

55. The risk is so prevalent for healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[41] *Id.*

[42] *2020 Internet Crime Report*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited July 24, 2024).

[43] *2021 DBIR Master's Guide*, VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited July 24, 2024).

"credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[44] The Cybersecurity and Infrastructure Security Agency ("CISA"), the Department of Health and Human Services ("HHS"), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[45]

56. There are two primary ways to mitigate the risk of stolen credentials: user education and technical security barriers. User education is the process of making employees or other users of a network aware of common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients.

57. From a technical perspective, companies can also greatly reduce the flow of fraudulent e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework ("SPF") (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail ("DKIM") (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance ("DMARC"), which "builds on the widely

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[44] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY, https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited July 24, 2024) ("CISA Guide").

[45] *Id.*

deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[46]

58. Additionally, because the goal of these schemes is to gain an employee's login credentials in order to access a company's network, there are industry-standard measures that companies can implement to greatly reduce unauthorized access, even if an individual's login credentials are disclosed, such as multi-factor authentication (a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login). Thus, even if hackers obtain an employee's username and password, access to the company's system is thwarted because they do not have access to the additional authentication methods.

59. Similarly, companies housing sensitive data must implement adequate "network segmentation," which is the practice of dividing a larger network into several smaller subnetworks that are each isolated from one another to provide enhanced security. For example, hackers that gain access to an unsegmented network (commonly through phishing) can move laterally across the network to access databases containing valuable assets such as sensitive personal information or financial records. Malicious lateral movement can be difficult to detect because it oftentimes appears as normal network traffic. By implementing adequate network segmentation, companies can prevent even those hackers who already gained a foothold in their network from moving across databases to access their most sensitive data.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[46] *Id.*

60. Network segmentation is commonly used in conjunction with the principle of least privilege ("POLP"), which is a security practice that limits employees' privileges to the minimum necessary to perform the job or task. In an IT environment, adhering to POLP reduces the risk of hackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.[47] In an example given by security software provider Digital Guardian: "an employee whose job is to enter info into a database only needs the ability to add records to that database. If malware infects that employee's computer or if the employee clicks a link in a phishing email, the malicious attack is limited to making database entries. If that employee has root access privileges, however, the infection can spread system-wide."[48]

61. This is precisely why approximately 67% of targeted malware and stolen credential schemes are directed at individual contributors and lower-level management personnel.[49]

62. In addition to mitigating the risk of stolen credentials, the CISA guidance encourages organizations to prevent unauthorized access by:

a. Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[47] Nate Lord, *What is the Prinicple of Least Privilge (POLP)?*, DIGITAL GUARDIAN (May 6, 2023), https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance.

[48] *Id.*

[49] *Jessica Davis*, *Pharmaceutical Companies Most Targeted Industry by Cybercriminals*, HEALTH IT SECURITY (Nov. 30, 2018), https://web.archive.org/web/20230102100837/https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-industry-by-cybercriminals.

b. Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;

c. Ensuring devices are properly configured and that security features are enabled;

d. Employing best practices for use of Remote Desktop Protocol ("RDP") as threat actors often gain initial access to a network through exposed and poorly secured remote services; and

e. Disabling operating system network file sharing protocol known as Server Message Block ("SMB") which is used by threat actors to travel through a network to spread malware or access sensitive data.[50]

63. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[51]

64. Despite holding the PHI of millions of patients, American Vision failed to adhere to these recommended best practices. Indeed, had American Vision implemented common sense security measures like network segmentation and POLP, the hackers never could have accessed millions of patient files and the Data Breach would have been prevented or been much

[50] CISA Guide at 4.
[51] *Id.* at 5.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

smaller in scope. American Vision also lacked the necessary safeguards to detect and prevent phishing attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred. The Ophthalmologist Defendants are equally responsible by partnering with American Vision and sharing sensitive information of millions of individuals with American Vision without overseeing its data security protocols or ensuring American Vision was equipped to protect highly sensitive PII/PHI.

65. Since the Data Breach, American Vision stated that "[w]e continue to take preventative actions to further safeguard our systems."[52] But American Vision, like any entity in the healthcare industry its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files. American Vision's below-industry-standard procedures and policies is inexcusable given its knowledge that it was a prime target for cyberattacks. Further, such vague statements are insufficient to demonstrate that American Vision actually fixed its data security issues. Thus, upon information and belief, Plaintiffs' and Class Members' PII/PHI remains unsecure and is thus susceptible to further unauthorized disclosure.

66. Defendants have done little to remedy the Data Breach. Although American Vision offered some victims credit monitoring and identity related services, such services cannot prevent identity theft or fraud and are wholly insufficient to compensate Plaintiffs and Class Members for the injuries caused by the Data Breach.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[52] https://oag.ca.gov/system/files/AVP%20Enclosures_0.pdf (last visited Aug. 1, 2024).

67. There is little doubt that the purpose of the Data Breach was to misuse stolen data for financial gain. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully "***obtained*** personal information" meaning it was exfiltrated and will be published or sold for financial gain.[53]

68. As the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[54]

69. Thus, upon information and belief, Plaintiffs' and the Class's stolen PII/PHI has already been published or sold by cybercriminals on the Dark Web or other underground markets.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

70. Because of Defendants' failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. losing the value of the explicit and implicit promises of data security;

c. the unconsented disclosure and publication of their PII/PHI;

[53] *Id*. (emphasis added).

[54] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendants' possession—and is thus at risk for futures breaches so long as Defendants fail to take appropriate measures to protect the PII/PHI.

71. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

72. The value of Plaintiffs and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

73. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

74. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

75. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

76. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

77. A similar issue arises in the wake of a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[55] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[56]

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[55] *Fifth Annual Study on Medical Identity Theft,* PONEMON INSTITUTE (Feb. 2015), https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 ("Ponemon Study").

[56] *Id.* at 9.

78. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[57]

79. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[58]

80. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because the Health Insurance Portability and Accountability Act's ("HIPAA") regulations require the victim to be personally involved in the resolution of the crime.[59] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[60]

81. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[57] *Id.* at 2.
[58] *Id.* at 14.
[59] *Id.* at 1.
[60] *Id.*

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

medical records and healthcare statements. For example, the Federal Trade Commission ("FTC") notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- Receive information from their health plan that they have reached their limit on bene-fits; or
- Be denied insurance because their medical records show a condition they do not have.[61]

82. Perhaps most dangerous, however, is the potential for misdiagnoses or treatment. According to Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance, "About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft." [62] This echoes the Ponemon study, which notes that "many

[61] *Medical Identity Theft, FAQs for Health Care Providers and Health Plans,* FTC.GOV, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faqhealth-care-healthplan.pdf (last visited July 30, 2024).
[62] Michelle Andrews, *The Rise of Medical Identity Theft*, CONSUMER REPORTS, https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited July 30, 2024).

respondents are at risk for further theft or errors in healthcare records that could jeopardize medical treatments and diagnosis."[63]

83. According to a Consumer Reports article entitled *The Rise of Medical Identity Theft*, this outcome "isn't a hypothetical problem" as the "long tail on medical identity theft can create havoc in victims' lives."[64] As one example, a pregnant woman reportedly used a victim's medical identity to pay for maternity care at a nearby hospital. When the infant was born with drugs in her system, the state threatened to take the *victim's* four children away—not realizing her identity had been stolen. The victim ultimately had to submit to a DNA test to remove her name from the infant's birth certificate, but it took years to get her medical records corrected.[65]

84. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[66] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[67] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[63] Ponemon Study at 1.
[64] Michelle Andrews, *The Rise of Medical Identity Theft*, CONSUMER REPORTS, https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited July 30, 2024).
[65] *Id.*
[66] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[67] *Id.*

85. Many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, medical-related identity theft and fraud. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and healthcare statements, checking credit reports, and spending time and effort searching for unauthorized activity.

86. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.[68]

[68] *Identity Theft: The Aftermath 2017*, ITRC, https://www.idtheftcenter.org/wpcontent/uploads/images/page-docs/Aftermath_2017.pdf (last visited July 30, 2024).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

87. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[69]

88. The unauthorized disclosure of the sensitive PHI to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[70]

89. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent

[69] *Id.*

[70] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

90. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. the unconsented disclosure of confidential information to a third party;

b. losing the value of the explicit and implicit promises of data security;

c. identity theft and fraud resulting from the theft of their PII/PHI;

d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

e. anxiety, emotional distress, and loss of privacy;

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PHI being in the possession of one or many unauthorized third parties.

91. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

92. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office ("GAO"), which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[71]

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[71] *PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, GAO, http://www.gao.gov/new.items/d07737.pdf (last visited July 30, 2024).

93. Plaintiffs and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[72]

94. Because of the value consumers place on data privacy and security, healthcare providers with robust data security practices are viewed more favorably by patients and can command higher prices than those who do not. Consequently, had patients known the truth about Defendants' data security practices—that they did not adequately protect and store their PII/PHI —they would not have sought medical care from Defendants or would have paid significantly less for such medical services. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with American Vision because they paid for the value of services they did not receive.

95. Plaintiffs and Class Members have a direct interest in Defendants' promises and duties to protect their PII/PHI, *i.e.*, that Defendants *not increase* their risk of identity theft and fraud. Because Defendants failed to live up to their promises and duties in this respect, Plaintiffs and Class Members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Defendants'

[72] *BEYOND THE BOTTOM LINE: THE REAL COST OF DATA BREACHES*, FIREEYE, https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf (last visited July 30, 2024).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

wrongful conduct. Through this remedy, Plaintiffs and Class Members seek to restore themselves and class members as close to the same position as they would have occupied but for Defendants' wrongful conduct, namely its failure to adequately protect Plaintiffs' and Class Members' PII/PHI.

96. Plaintiffs and Class Members further seek to recover the value of the unauthorized access to their PII/PHI permitted through Defendants' wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII/PHI is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and Class Members have a protectible property interest in their PII/PHI; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

97. Defendants' failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

steps to mitigate the harm caused by the Data Breach. Furthermore, American Vision's notification letter did not explain the precise nature of the attack, the identity of the hackers, or the number of individuals affected. Defendants' decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By waiting months to disclose the Data Breach, Defendants prevented victims from taking meaningful, proactive, and targeted mitigation measures that could help protect them from harm.

98. Because Defendants continue to hold the Plaintiffs' and Class Members' PII/PHI, Plaintiffs and Class Members have an interest in ensuring that their PII/PHI is secured and not subject to further theft.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Defendants Knew—Or Should Have Known—of the Risk of a Data Breach

99. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

100. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[73] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[74] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[75]

---

[73] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[74] *Id.*

[75] *Id.*

101. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[76]

102. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants.

Defendants Failed to Follow FTC Guidelines

103. According to the FTC, the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendants—should use to protect against unlawful data exposure.

104. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[77] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

[76] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (subscription required) (last visited July 24, 2024).

[77] *Protecting Personal Information: A Guide for Business,* FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

105. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

106. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

107. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

108. In short, Defendants' failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former employees' and patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

109. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendants. These industry standards include: educating all employees; requiring strong passwords; employing multi-layer security, including firewalls, anti-virus, and anti-malware software; implementing encryption (making data unreadable without a key); enabling multi-factor authentication; backing up data; and limiting which employees can access sensitive data.

110. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protecting against any possible communication system; and training staff regarding critical points.

111. Defendants also failed to meet the minimum standards of any of the following frameworks: the National Institute of Standards and Technolgoy's ("NIST") Cybersecurity Framework Version 1.1, and the Center for Internet Security's Critical Security Controls ("CIS CSC"), which are all established standards in reasonable cybersecurity readiness.

112. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendants opened the door to the criminals—thereby causing the Data Breach.

Defendants Violated HIPAA

113. Upon information and belief, because Defendants receive, maintain, and handle patient PHI, Defendants qualify as covered entities under HIPAA, 42 U.S.C. § 1302d, *et seq.*

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

114. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[78]

115. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[79]

116. The Data Breach itself resulted from a combination of inadequacies showing Defendants failed to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[78] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[79] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Defendants' workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

117. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

Plaintiffs' Experiences

Plaintiff Linda Hulewat

118. For purposes of receiving medical treatment at SWEC, Plaintiff Hulewat was required to provide her highly sensitive information, including her name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

119. SWEC also maintained Plaintiff Hulewat's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. SWEC shared Plaintiff Hulewat's PII/PHI with American Vision in connection with her treatment.

120. Plaintiff Hulewat received a notice letter from Defendant American Vision dated February 15, 2024, informing her of the Data Breach and the exposure of her PII/PHI.

121. The notice letter informed Plaintiff Hulewat that her name, contact information, date of birth, medical information and insurance information was potentially compromised in the Data Breach.

122. Plaintiff Hulewat only allowed SWEC to maintain, store, and use her PII/PHI because she believed SWEC would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

overseen by SWEC and who likewise implemented reasonable security measures to protect PII/PHI.

123. In the instant that her PII/PHI was accessed and obtained by a third party without her consent or authorization, Plaintiff Hulewat suffered injury from a loss of privacy.

124. Plaintiff Hulewat has been further injured by the damages to and diminution in value of her PII/PHI—a form of intangible property that Plaintiff Hulewat entrusted to Defendants. This information has inherent value that Plaintiff Hulewat was deprived of when her PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

125. Plaintiff Hulewat has experienced numerous targeted scam and spam calls and texts in the time after the Data Breach and as a result of the Data Breach.

126. The Data Breach has also caused Plaintiff Hulewat to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of criminals.

127. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Hulewat has undertook mitigation activities including researching and verifying the legitimacy of the Data Breach as well as monitoring her financial accounts for unusual activity.

128. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Hulewat to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

129. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Hulewat to suffer stress, fear, and anxiety.

130. Plaintiff Hulewat has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Karen Foti Williams

131. For purposes of receiving medical treatment at SWEC, Plaintiff Williams was required to provide her highly sensitive information, including her name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

132. SWEC also maintained Plaintiff Williams' patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. SWEC shared Plaintiff Williams's PII/PHI with American Vision in connection with her treatment

133. Plaintiff Williams received a notice letter from Defendant American Vision dated February 15, 2024, informing her of the Data Breach and the exposure of her PII/PHI.

134. The notice letter informed Plaintiff Williams that her name, contact information, date of birth, medical information and insurance information was potentially compromised in the Data Breach.

135. Plaintiff Williams only allowed SWEC to maintain, store, and use her PII/PHI because she believed SWEC would implement adequate security measures to protect it,

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

including only sharing it with third parties whose data security practices were vetted and overseen by SWEC and who likewise implemented reasonable security measures to protect PII/PHI.

136. In the instant that her PII/PHI was accessed and obtained by a third party without her consent or authorization, Plaintiff Williams suffered injury from a loss of privacy.

137. Plaintiff Williams has been further injured by the damages to and diminution in value of her PII/PHI—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff Williams was deprived of when her PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

138. Plaintiff Williams has experienced numerous targeted scam and spam calls and texts in the time after the Data Breach and as a result of the Data Breach.

139. The Data Breach has also caused Plaintiff Williams to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of criminals.

140. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Williams checked her bank account daily for the first month after she received the data breach notice. She currently checks her bank account on a weekly basis, spending at least five to ten minutes per session. She also reviews her account statements carefully, which requires approximately one hour of her time each month.

141. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Williams to spend significant time dealing with issues related to the Data

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

142. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Williams to suffer stress, fear, and anxiety.

143. Plaintiff Williams has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Ralph Gallegos

144. For purposes of receiving medical treatment at SWEI, Plaintiff Gallegos was required to provide his highly sensitive information, including his name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

145. SWEI also maintained Plaintiff Gallegos's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. SWEI shared Plaintiff Gallegos' PII/PHI with American Vision in connection with his treatment.

146. Plaintiff Gallegos received a notice letter from Defendant American Vision dated February 15, 2024, informing him of the Data Breach and the exposure of his PII/PHI.

147. The notice letter informed Plaintiff Gallegos that his name, contact information, date of birth, certain medical information, and insurance information was potentially compromised in the Data Breach.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

148. Plaintiff Gallegos only allowed SWEI to maintain, store, and use his PII/PHI because he believed SWEI would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by SWEI and who likewise implemented reasonable security measures to protect PII/PHI.

149. In the instant that his PII/PHI was accessed and obtained by a third party without his consent or authorization, Plaintiff Gallegos suffered injury from a loss of privacy.

150. Plaintiff Gallegos has been further injured by the damages to and diminution in value of his PII/PHI—a form of intangible property that Plaintiff Gallegos entrusted to Defendants. This information has inherent value that Plaintiff Gallegos was deprived of when his PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

151. Upon information and belief, Plaintiff Gallegos' PII/PHI has already been stolen and misused as he experienced incidents of increased targeted scam and spam calls after the Data Breach. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Gallegos' life, and specifically caused strain on him as a direct result of the Data Breach.

152. The Data Breach has also caused Plaintiff Gallegos to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII/PHI being placed in the hands of criminals.

153. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Gallegos has experienced lost time as a result of the Data Breach, as he has to monitor his accounts for potential fraudulent activity.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

154. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Gallegos to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

155. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Gallegos to suffer stress and fear that his identity will be stolen in the future.

156. Plaintiff Gallegos has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Michael Martinez

157. For purposes of receiving medical treatment at SWEC, Plaintiff Martinez was required to provide his highly sensitive information, including his name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

158. SWEC also maintained Plaintiff Martinez's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. SWEC shared Plaintiff Martinez's PII/PHI with American Vision in connection with his treatment.

159. Plaintiff Martinez received a notice letter from Defendant American Vision dated February 15, 2024, informing him of the Data Breach and the exposure of his PII/PHI.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

160. The notice letter informed Plaintiff Martinez that his name, contact information, date of birth, medical information, and insurance information was potentially compromised in the Data Breach.

161. Plaintiff Martinez only allowed SWEC to maintain, store, and use his PII/PHI because he believed SWEC would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by SWEC and who likewise implemented reasonable security measures to protect PII/PHI.

162. In the instant that his PII/PHI was accessed and obtained by a third party without his consent or authorization, Plaintiff Martinez suffered injury from a loss of privacy.

163. Plaintiff Martinez has been further injured by the damages to and diminution in value of his PII/PHI—a form of intangible property that Plaintiff Martinez entrusted to Defendants. This information has inherent value that Plaintiff Martinez was deprived of when his PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

164. Upon information and belief, Plaintiff Martinez's PII/PHI has already been stolen and misused as he has experienced incidents of fraud and identity theft so far because he received notifications from Experian and Credit Karma after the Data Breach that his PII/PHI was stolen and available on the Dark Web, and he received a notification from McAfee of potential fraud. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Martinez's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

165. Furthermore, Plaintiff Martinez has experienced an increase in targeted scam and spam calls and texts using his PII/PHI in the time after the Data Breach and as a result of the Data Breach.

166. The Data Breach has also caused Plaintiff Martinez to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII/PHI being placed in the hands of criminals.

167. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Martinez has spent time researching the Data Breach, reviewing credit reports, and reviewing available credit monitoring services to protect his PII/PHI.

168. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Martinez to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

169. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

170. Plaintiff Martinez has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Lynnae Anderson

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

171. For purposes of receiving medical treatment at SWEC, Plaintiff Anderson was required to provide her highly sensitive information, including her name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

172. SWEC also maintained Plaintiff Anderson's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. SWEC shared Plaintiff Anderson's PII/PHI with American Vision in connection with her treatment.

173. Plaintiff Anderson received a notice letter from Defendant American Vision dated February 15, 2024, informing her of the Data Breach and the exposure of her PII/PHI.

174. The notice letter informed Plaintiff Anderson that her name, contact information, date of birth, medical information, and insurance information was potentially compromised in the Data Breach.

175. Plaintiff Anderson only allowed SWEC to maintain, store, and use her PII/PHI because she believed SWEC would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by SWEC and who likewise implemented reasonable security measures to protect PII/PHI.

176. In the instant that her PII/PHI was accessed and obtained by a third party without her consent or authorization, Plaintiff Anderson suffered injury from a loss of privacy.

177. Plaintiff Anderson has been further injured by the damages to and diminution in value of her PII/PHI—a form of intangible property that Plaintiff Anderson entrusted to Defendants. This information has inherent value that Plaintiff Anderson was deprived of when

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

her PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

178. Upon information and belief, Plaintiff Anderson's PII/PHI has already been stolen and misused as she has experienced incidents of fraud and identity theft so far because she received notifications from Credit Karma after the Data Breach that her PII/PHI was stolen and available on the Dark Web. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Anderson's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

179. Furthermore, Plaintiff Anderson has experienced an increase in targeted scam and spam calls and texts using her PII/PHI in the time after the Data Breach and as a result of the Data Breach.

180. The Data Breach has also caused Plaintiff Anderson to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of criminals.

181. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Anderson has spent time researching the Data Breach, reviewing credit reports, and reviewing notifications about changes in her credit reports.

182. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Anderson to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

183. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Anderson to suffer stress, fear, and anxiety.

184. Plaintiff Anderson has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Candia Franklin

185. For purposes of receiving medical treatment at Barnet, Plaintiff Franklin was required to provide her highly sensitive information, including her name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

186. Barnet also maintained Plaintiff Franklin's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. Barnet shared Plaintiff Franklin's PII/PHI with American Vision in connection with her treatment.

187. Plaintiff Franklin received a notice letter from Defendant American Vision in approximately early 2024 informing her of the Data Breach and the exposure of her PII/PHI.

188. The notice letter informed Plaintiff Franklin that her PII/PHI was potentially compromised in the Data Breach.

189. Plaintiff Franklin only allowed Barnet to maintain, store, and use her PII/PHI because she believed Barnet would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

overseen by Barnet and who likewise implemented reasonable security measures to protect PII/PHI.

190. In the instant that her PII/PHI was accessed and obtained by a third party without her consent or authorization, Plaintiff Franklin suffered injury from a loss of privacy.

191. Plaintiff Franklin has been further injured by the damages to and diminution in value of her PII/PHI—a form of intangible property that Plaintiff Franklin entrusted to Defendants. This information has inherent value that Plaintiff Franklin was deprived of when her PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

192. Furthermore, Plaintiff Franklin has experienced a significant increase in the number of targeted scam and spam calls she receives as a direct result of the Data Breach. Prior to the Data Breach, Plaintiff Franklin received approximately two targeted scam and spam phone calls per week. Since the Data Breach, she now receives approximately 20 targeted scam and spam calls per week as a result of the Data Breach.

193. The Data Breach has also caused Plaintiff Franklin to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of criminals. Indeed, in the wake of the Data Breach, Plaintiff Franklin was alerted that her email address is now on the dark web.

194. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Franklin has spent dozens of hours responding to the Data Breach, including notifying the financial institutions with which she has accounts that her email address

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

is now on the dark web, creating a new email account, changing her registered email and login information with her financial institutions, and monitoring her accounts and statements for fraud.

195. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Franklin to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

196. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Franklin to suffer stress, fear, and anxiety.

197. Plaintiff Franklin has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Marie Therese Montoya

198. For purposes of receiving medical treatment at Flagstaff Vision and Costco Vision, Plaintiff Montoya was required to provide her highly sensitive information, including her name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

199. Flagstaff Vision and Costco Vision also maintained Plaintiff Montoya's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. On information and belief,

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Flagstaff Vision and Costco Vision shared Plaintiff Montoya's PII/PHI with American Vision in connection with her treatment.

200. Plaintiff Montoya received a notice letter from Defendant American Vision on February 15, 2024, informing her of the Data Breach and the exposure of her PII/PHI.

201. The notice letter informed Plaintiff that her PII/PHI was potentially compromised in the Data Breach.

202. Plaintiff only allowed Flagstaff Vision and Costco Vision to maintain, store, and use her PII/PHI because she believed Flagstaff Vision and Costco Vision would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by Flagstaff Vision and Costco Vision and who likewise implemented reasonable security measures to protect PII/PHI. Had Plaintiff Montoya known that American Vision did not have adequate data security practices to protect her PII/PHI, she would not have allowed it to be shared with American Vision.

203. In the instant that her PII/PHI was accessed and obtained by a third party without her consent or authorization, Plaintiff Montoya suffered injury from a loss of privacy.

204. Plaintiff Montoya has been further injured by the damages to and diminution in value of her PII/PHI—a form of intangible property that Plaintiff Montoya entrusted to Defendants. This information has inherent value that Plaintiff Montoya was deprived of when her PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

205. The Data Breach has also caused Plaintiff Montoya to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

theft, and misuse resulting from her PII/PHI being placed in the hands of criminals.

206. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Montoya has spent multiple hours responding to the Data Breach, including reviewing her financial accounts for unusual activity, contacting credit bureaus, and researching and verifying the legitimacy of the Data Breach.

207. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Montoya to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

208. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Montoya to suffer stress, fear, and anxiety.

209. Plaintiff Montoya has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Charles Peterson

210. For purposes of receiving medical treatment at Barnet, Plaintiff Peterson was required to provide his highly sensitive information, including his name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

211. Barnet also maintained Plaintiff Peterson's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

and clinical treatment information. Barnet shared Plaintiff Peterson's PII/PHI with American Vision in connection with his treatment.

212. Plaintiff Peterson received a notice letter from Defendant American Vision dated February 15, 2024, informing him of the Data Breach and the exposure of his PII/PHI.

213. The notice letter informed Plaintiff Peterson that his name, contact information, date of birth, medical information, and health insurance were potentially compromised in the Data Breach.

214. Plaintiff Peterson only allowed Barnet to maintain, store, and use his PII/PHI because he believed Barnet would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by SWEC and who likewise implemented reasonable security measures to protect PII/PHI.

215. In the instant that his PII/PHI was accessed and obtained by a third party without his consent or authorization, Plaintiff Peterson suffered injury from a loss of privacy.

216. Plaintiff Peterson has been further injured by the damages to and diminution in value of his PII/PHI—a form of intangible property that Plaintiff Peterson entrusted to Defendants. This information has inherent value that Plaintiff Peterson was deprived of when his PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

217. The Data Breach has also caused Plaintiff Peterson to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII/PHI being placed in the hands of criminals.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

218. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Peterson spent multiple hours responding to the Data Breach. This time has consisted of monitoring Plaintiff Peterson's accounts for fraudulent charges, browsing the Internet discover developments about the Data Breach, and speaking with and coordinating with Plaintiffs' counsel about the ongoing litigation.

219. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Peterson to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

220. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Peterson to suffer stress over his loss of confidence in Defendants' ability to protect his PII/PHI from unauthorized access and use and fear over the potential for malicious actors to use his PII/PHI for identity theft.

221. Plaintiff Peterson has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Robert Kirk

222. For purposes of receiving medical treatment at Barnet, Plaintiff Kirk was required to provide his highly sensitive information, including his name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

223. Barnet also maintained Plaintiff Kirk's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. Barnet shared Plaintiff Kirk's PII/PHI with American Vision in connection with his treatment.

224. Plaintiff Kirk received a notice letter from Defendant American Vision informing him of the Data Breach and the exposure of his PII/PHI.

225. The notice letter informed Plaintiff Kirk that his PII/PHI was potentially compromised in the Data Breach.

226. Plaintiff Kirk only allowed Barnet to maintain, store, and use her PII/PHI because she believed Barnet would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by Barnet and who likewise implemented reasonable security measures to protect PII/PHI.

227. In the instant that his PII/PHI was accessed and obtained by a third party without his consent or authorization, Plaintiff Kirk suffered injury from a loss of privacy.

228. Plaintiff Kirk has been further injured by the damages to and diminution in value of his PII/PHI—a form of intangible property that Plaintiff Kirk entrusted to Defendants. This information has inherent value that Plaintiff Kirk was deprived of when his PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

229. Upon information and belief, Plaintiff Kirk's PII/PHI has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of fraudulent charges on his debit card in July 2024. These actions by unauthorized criminal third

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

parties have detrimentally impacted Plaintiff Kirk's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

230. Furthermore, Plaintiff Kirk has experienced additional difficulties and injury resulting from the identity theft and fraud he experienced as a result of the Data Breach. Plaintiff Kirk's bank closed his debit card and reissued a new card after he experienced fraudulent charges in July 2024. As a result, Plaintiff Kirk's automatic payment for his phone service failed, and he was forced to pay a fee of approximately $50 to reinstate his phone service.

231. The Data Breach has also caused Plaintiff Kirk to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII/PHI being placed in the hands of criminals.

232. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Kirk to suffer stress, fear, and anxiety.

233. Plaintiff Kirk has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Lynda Israel

234. For purposes of receiving medical treatment at Wellish, Plaintiff Israel was required to provide her highly sensitive information, including her name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

235. Wellish also maintained Plaintiff Israel's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

and clinical treatment information. Wellish shared Plaintiff Israel's PII/PHI with American Vision in connection with her treatment.

236. Plaintiff Israel received, on February 22, 2024, a notice letter from Defendant American Vision dated February 15, 2024, informing her of the Data Breach and the exposure of her PII/PHI.

237. The notice letter informed Plaintiff Israel that her name, contact information, date of birth, insurance information, and medical information such as clinical records, details about services received, and medication and prescription information, were potentially compromised in the Data Breach.

238. Plaintiff Israel only allowed Wellish to maintain, store, and use her PII/PHI because she believed Wellish would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by Wellish and who likewise implemented reasonable security measures to protect PII/PHI.

239. In the instant that her PII/PHI was accessed and obtained by a third party without her consent or authorization, Plaintiff Israel suffered injury from a loss of privacy.

240. Plaintiff Israel has been further injured by the damages to and diminution in value of her PII/PHI—a form of intangible property that Plaintiff Israel entrusted to Defendants. This information has inherent value that Plaintiff Israel was deprived of when her PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

241. Plaintiff Israel takes her data security seriously and she is proactive about keeping her information safe and preventing identity theft. She diligently monitors her credit reports, froze her credit, and she has set up filters on her phone and email to reduce the overwhelming amount of targeted scam and spam calls, texts, and emails that she receives. Despite these measures, she has still experienced a rise in the number of targeted scam and spam calls as a result of the Data Breach.

242. The Data Breach has also caused Plaintiff Israel to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of criminals.

243. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Israel to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

244. As a result of the Data Breach and the increased imminent risk of future harm, Plaintiff Israel upgraded her LifeLock subscription to the highest level, which costs her approximately $400 per year.

245. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Israel to suffer stress, fear, and anxiety.

246. Plaintiff Israel has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

safeguarded from future breaches.

Plaintiff Latricia Pelt

247. For purposes of receiving medical treatment at VisionWorks, Plaintiff Pelt was required to provide her highly sensitive information, including her name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

248. VisionWorks also maintained Plaintiff Pelt's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. On information and belief, VisionWorks shared Plaintiff Pelt's PII/PHI with American Vision in connection with her treatment.

249. Plaintiff Latricia Pelt received a notice letter from Defendant American Vision dated February 15, 2024, informing her of the Data Breach and the exposure of her PII/PHI.

250. The notice letter informed Plaintiff Pelt that her name, contact information, date of birth, medical information and insurance information was potentially compromised in the Data Breach.

251. Plaintiff Latricia Pelt only allowed VisionWorks to maintain, store, and use her PII/PHI because she believed VisionWorks would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by VisionWorks and who likewise implemented reasonable security measures to protect PII/PHI. Had Plaintiff Latricia Pelt known that American Vision did not have adequate data security practices to protect her PII/PHI, she would not have allowed it to be shared with American Vision.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

252. In the instant that her PII/PHI was accessed and obtained by a third party without her consent or authorization, Plaintiff Pelt suffered injury from a loss of privacy.

253. Plaintiff Pelt has been further injured by the damages to and diminution in value of her PII/PHI—a form of intangible property that Plaintiff Pelt entrusted to Defendants. This information has inherent value that Plaintiff Pelt was deprived of when her PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

254. Upon information and belief, Plaintiff Pelt's PII/PHI has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of unauthorized credit card charges and credit inquiries as recently as July 2024. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Pelt's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

255. Furthermore, in the time after the Data Breach, Plaintiff Pelt has experienced a significant increase in not only targeted scam and spam calls, but scam callers who already know her PII/PHI, as a result of the Data Breach.

256. The Data Breach has also caused Plaintiff Pelt to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of criminals.

257. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Pelt has spent countless hours monitoring her accounts, freezing her credit and registering for credit notification services.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

258. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Pelt to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

259. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Pelt to suffer stress, fear, and anxiety.

260. Plaintiff Pelt has a continuing interest in ensuring that Plaintiff Pelt's PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Barry Pelt

261. For purposes of receiving medical treatment at Barnet and VisionWorks, Plaintiff Pelt was required to provide his highly sensitive information, including his name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

262. Barnet and VisionWorks also maintained Plaintiff Pelt's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. Barnet and VisionWorks shared Plaintiff Pelt's PII/PHI with American Vision in connection with his treatment.

263. Plaintiff Barry Pelt only allowed Barnet and VisionWorks to maintain, store, and use his PII/PHI because he believed Barnet and VisionWorks would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by Barnet and VisionWorks and who likewise implemented

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

reasonable security measures to protect PII/PHI. Had Plaintiff Barry Pelt known that American Vision did not have adequate data security practices to protect his PII/PHI, he would not have allowed it to be shared with American Vision.

264. In the instant that his PII/PHI was accessed and obtained by a third party without his consent or authorization, Plaintiff Pelt suffered injury from a loss of privacy.

265. Plaintiff Pelt has been further injured by the damages to and diminution in value of his PII/PHI—a form of intangible property that Plaintiff Pelt entrusted to Defendants. This information has inherent value that Plaintiff Pelt was deprived of when his PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

266. In the time after the Data Breach, Plaintiff Pelt has experienced a significant increase in not only targeted scam and spam calls, but scam callers who already know his PII/PHI, as a result of the Data Breach.

267. The Data Breach has also caused Plaintiff Pelt to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII/PHI being placed in the hands of criminals.

268. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Pelt has subscribed to credit monitoring alerts and spends time monitoring his accounts for fraudulent activity.

269. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Pelt to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

270. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Pelt to suffer stress, fear, and anxiety.

271. Plaintiff Pelt has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Ken Waters

272. For purposes of receiving medical treatment at SWEC, Plaintiff Waters was required to provide his highly sensitive information, including his name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

273. SWEC also maintained Plaintiff Waters's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. SWEC shared Plaintiff Waters' PII/PHI with American Vision in connection with his treatment.

274. Plaintiff Waters received a notice letter from Defendant American Vision dated February 15, 2024 informing him of the Data Breach and the exposure of his PII/PHI.

275. The notice letter informed Plaintiff Waters that his name, contact information, date of birth, medical information, and health insurance was potentially compromised in the Data Breach.

276. Plaintiff Waters only allowed SWEC to maintain, store, and use his PII/PHI because he believed SWEC would implement adequate security measures to protect it,

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

including only sharing it with third parties whose data security practices were vetted and overseen by SWEC and who likewise implemented reasonable security measures to protect PII/PHI.

277. In the instant that his PII/PHI was accessed and obtained by a third party without his consent or authorization, Plaintiff Waters suffered injury from a loss of privacy.

278. Plaintiff Waters has been further injured by the damages to and diminution in value of his PII/PHI—a form of intangible property that Plaintiff Waters entrusted to Defendants. This information has inherent value that Plaintiff Waters was deprived of when his PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

279. Upon information and belief, Plaintiff Waters' PII/PHI has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of an individual opening a credit account in his name in November 2023 after a hard inquiry was run on his credit and an individual attempting to apply for a credit card in his name in February 2024.These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Waters' life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

280. Furthermore, Plaintiff Waters has experienced an increased number of targeted scam and spam calls and emails as a result of the Data Breach. Plaintiff Waters noticed that the number of targeted scam and spam calls dramatically increased after the Data Breach as opposed to the amount he received before the Data Breach.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

281. The Data Breach has also caused Plaintiff Waters to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII/PHI being placed in the hands of criminals.

282. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Waters has been required to spend his valuable time and effort in an attempt to mitigate the misuse of his PII/PHI, including time spend freezing his credit and logging in and reviewing his various accounts for suspicious activity. Plaintiff Waters has spent dozens of hours engaging in these mitigation efforts.

283. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Waters to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his/her/their accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

284. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Waters to suffer stress, fear, and anxiety about future identity theft.

285. Plaintiff Waters has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Brenda Moreno-Decerra

286. For purposes of receiving medical treatment at SWEC , Plaintiff Moreno-Decerra was required to provide her highly sensitive information, including her name, date of birth,

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

SSN, medical history, address, phone number, insurance information and a photo ID.

287. SWEC also maintained Plaintiff's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. SWEC shared Plaintiff Moreno-Decerra's PII/PHI with American Vision in connection with her treatment.

288. Plaintiff Moreno-Decerra received a notice letter from Defendant American Vision dated February 15, 2024, informing her of the Data Breach and the exposure of her PII/PHI.

289. The notice letter informed Plaintiff Moreno-Decerra that her name, contact information, date of birth, medical information, and health insurance was potentially compromised in the Data Breach.

290. Plaintiff Moreno-Decerra only allowed SWEC to maintain, store, and use her PII/PHI because she believed SWEC would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by SWEC and who likewise implemented reasonable security measures to protect PII/PHI.

291. In the instant that her PII/PHI was accessed and obtained by a third party without her consent or authorization, Plaintiff Moreno-Decerra suffered injury from a loss of privacy.

292. Plaintiff Moreno-Decerra has been further injured by the damages to and diminution in value of her PII/PHI—a form of intangible property that Plaintiff Moreno-Decerra entrusted to Defendants. This information has inherent value that Plaintiff Moreno-Decerra was deprived of when her PII/PHI was placed on a publicly accessible database,

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

293. Upon information and belief, Plaintiff Moreno-Decerra's PII/PHI has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of fraudulent credit card charges in May 2024. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Moreno-Decerra's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

294. Furthermore, Plaintiff Moreno-Decerra has experienced an increased number of targeted scam and spam calls and emails as a result of the Data Breach. Plaintiff Moreno-Decerra noticed that the number of targeted scam and spam calls dramatically increased after the Data Breach as opposed to the amount she received before the Data Breach.

295. The Data Breach has also caused Plaintiff Moreno-Decerra to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of criminals.

296. As a result of the actual harm she has suffered and the increased imminent risk of future harm Plaintiff Moreno-Decerra has been required to spend her valuable time verifying the legitimacy of the Data Breach Notice Letter, resolving the fraudulent credit card charges, changing her health insurance provider, and contacting the credit bureaus to place a fraud alert on her credit.

297. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Moreno-Decerra to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Letter, resolving the fraudulent credit card charges, changing her health insurance provider, and contacting the credit bureaus to place a fraud alert on her credit. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

298. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Moreno-Decerra to suffer stress, fear, and anxiety knowing that hackers accessed and likely exfiltrated her PII and that this information likely has been and will be used in the future for identity theft, fraud, and other nefarious purposes.

299. Plaintiff Moreno-Decerra has a continuing interest in ensuring that Plaintiff Moreno-Decerra's PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Robert Ahrensdorf

300. For purposes of receiving medical treatment at Barnet, Plaintiff Ahrensdorf was required to provide his highly sensitive information, including his name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

301. Barnet also maintained Plaintiff Ahrensdorf's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. Barnet shared Plaintiff Ahrensdorf's PII/PHI with American Vision in connection with his treatment.

302. Plaintiff Ahrensdorf received a notice letter from Defendant American Vision dated February 15, 2024, informing him of the Data Breach and the exposure of his PII/PHI.

303. The notice letter informed Plaintiff Ahrensdorf that his name, contact information, date of birth, medical information and insurance information was potentially

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

compromised in the Data Breach.

304. Plaintiff Ahrensdorf only allowed Barnet to maintain, store, and use his PII/PHI because he believed Barnet would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by Barnet and who likewise implemented reasonable security measures to protect PII/PHI.

305. In the instant that his PII/PHI was accessed and obtained by a third party without his consent or authorization, Plaintiff Ahrensdorf suffered injury from a loss of privacy.

306. Plaintiff Ahrensdorf has been further injured by the damages to and diminution in value of his PII/PHI—a form of intangible property that Plaintiff Ahrensdorf entrusted to Defendants. This information has inherent value that Plaintiff Ahrensdorf was deprived of when his PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

307. Plaintiff Ahrensdorf has experienced a dramatic increase in targeted scam and spam emails, calls, and texts since the Data Breach and as a result of the Data Breach.

308. The Data Breach has also caused Plaintiff Ahrensdorf to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII/PHI being placed in the hands of criminals.

309. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Ahrensdorf diligently checked his credit report and bank statements regularly following notice of the Data Breach. Plaintiff Ahrensdorf has spent multiple hours so far verifying the legitimacy of the Notice letter, checking his statements, securing and changing his passwords, and dealing with targeted scam and spam.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

310. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Ahrensdorf to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

311. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Ahrensdorf to suffer stress, fear, and anxiety.

312. Plaintiff Ahrensdorf has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff David Yeager

313. For purposes of receiving medical treatment at Barnet, Plaintiff Yeager was required to provide his highly sensitive information, including his name, date of birth, SSN, medical history, address, phone number, insurance information and a photo ID.

314. Barnet also maintained Plaintiff Yeager's patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information. Barnet shared Plaintiff Yeager's PII/PHI with American Vision in connection with his treatment.

315. Plaintiff Yeager received a notice letter from Defendant American Vision dated February 15, 2024, informing him of the Data Breach and the exposure of his PII/PHI.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

316. The notice letter informed Plaintiff Yeager that his name, contact information, date of birth, medical information and insurance information was potentially compromised in the Data Breach.

317. Plaintiff Yeager only allowed Barnet to maintain, store, and use his PII/PHI because he believed Barnet would implement adequate security measures to protect it, including only sharing it with third parties whose data security practices were vetted and overseen by Barnet and who likewise implemented reasonable security measures to protect PII/PHI.

318. In the instant that his PII/PHI was accessed and obtained by a third party without his consent or authorization, Plaintiff Yeager suffered injury from a loss of privacy.

319. Plaintiff Yeager has been further injured by the damages to and diminution in value of his PII/PHI—a form of intangible property that Plaintiff Yeager entrusted to Defendants. This information has inherent value that Plaintiff Yeager was deprived of when his PII/PHI was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

320. Upon information and belief, Plaintiff Yeager's PII/PHI has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of fraud on his debit card. In approximately March or April 2024, Plaintiff Yeager experienced unauthorized charges on his debit card. That debt card was the same one he used to pay for his eye care with Barnet. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Yeager's life as a whole, and specifically caused financial and emotional strain on him as a direct result of the Data Breach.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

321. Plaintiff Yeager has experienced a dramatic increase in targeted scam and spam emails, calls, and texts since the Data Breach and as a result of the Data Breach.

322. The Data Breach has also caused Plaintiff Yeager to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII/PHI being placed in the hands of criminals.

323. As a result of the Data Breach, Plaintiff Yeager made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Yeager has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff Yeager otherwise would have spent on other activities. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

324. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Yeager to suffer stress, fear, and anxiety.

325. Plaintiff Yeager has a continuing interest in ensuring that his PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

326. Plaintiffs seek relief in their individual capacity and as representatives of all others who are similarly situated. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs bring this action on behalf of themselves and the Class defined as:

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Nationwide Class: All individuals whose PII/PHI was compromised in the Data Breach announced by American Vision in February 2024.

327. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs also seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes, on behalf of separate State Subclasses, defined as:

Arizona Class: All individuals who are citizens of Arizona whose PII/PHI was compromised in the Data Breach announced by American Vision in February 2024.

Michigan Class: All individuals who are citizens of Michigan whose PII/PHI was compromised in the Data Breach announced by American Vision in February 2024.

Texas Class: All individuals who are citizens of Texas whose PII/PHI was compromised in the Data Breach announced by American Vision in February 2024.

Nevada Class: All individuals who are citizens of Nevada whose PII/PHI was compromised in the Data Breach announced by American Vision in February 2024.

The foregoing State Subclasses, together with the Nationwide Class, are referred to collectively as the "Class" herein. The State Subclasses, when referred to separately, are each referred to as "[STATE] Class."

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

328. Specifically excluded from the Class are Defendants; their officers and directors; any entity in which Defendants have a controlling interest; and any affiliate, legal representative, heir, or assign of Defendants. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

329. **Class Identity**: The members of the Class are readily identifiable and ascertainable. Defendants and/or their affiliates, among others, possess the information to identify and contact Class Members.

330. **Numerosity**: The members of the Class are so numerous that joinder of all of them is impracticable. Defendants' disclosures reveal that the Class contains nearly 2.4 million individuals whose PII/PHI was compromised in the Data Breach.

331. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class because all Class Members had their PII/PHI compromised in the Data Breach and were harmed as a result.

332. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no known interest antagonistic to those of the Class and their interests are aligned with Class Members' interests. Plaintiffs were subject to the same Data Breach as Class Members, suffered similar harms, and face similar threats due to the Data Breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including data breach cases involving multiple classes and data breach claims.

333. **Commonality and Predominance**: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

common questions predominate over any questions affecting only individual Class Members. The common questions of law and fact include, without limitation:

a. Whether Defendants owed Plaintiffs and Class Members a duty to implement and maintain reasonable security procedures and practices to protect their PII/PHI;

b. Whether Defendants received a benefit without proper restitution making it unjust for Defendants to retain the benefit without commensurate compensation;

c. Whether Defendants acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class Members' PII/PHI;

d. Whether Defendants violated its duty to implement reasonable security systems to protect Plaintiffs' and Class Members' PII/PHI;

e. Whether Defendants' breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class Members;

f. Whether Defendants adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

g. Whether Plaintiffs and Class Members are entitled to damages to pay for future protective measures like credit monitoring and monitoring for misuse of medical information;

h. Whether Defendants provided timely notice of the Data Breach to Plaintiffs and Class Members; and

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

i. Whether Class Members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

334. Defendants have engaged in a common course of conduct and Plaintiffs and Class Members have been similarly impacted by Defendants' failure to maintain reasonable security procedures and practices to protect patients' and employees' PII/PHI, as well as Defendants' failure to timely alert affected patients and employees to the Data Breach.

335. **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. Absent a class action, most if not all Class Members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses, Against American Vision)

336. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

337. American Vision owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PII/PHI within their control from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Further, American Vision owed a duty of care to Plaintiffs and Class Members to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the PII/PHI. American Vision acknowledged this duty in its HIPAA Notice of Privacy Practices, where it promised not to disclose this information without authorization.

338. American Vision's duty to use reasonable care in protecting PII/PHI arises as a result of the parties' relationship, as well as common law, state statutes, and federal law, including the HIPAA regulations described above and American Vision's own policies and promises regarding privacy and data security and Ariz. Stat. § 12-2292(A), which states that "all medical records and payment records, and the information contained in medical records and payment records, are privileged and confidential."

339. A "special relationship" exists between American Vision and the Plaintiffs and Class Members. American Vision entered into a "special relationship" with Plaintiffs and Class Members who (1) use American Vision's management services—either directly or indirectly through their respective Ophthalmologist Defendants that use those services on Plaintiffs' and Class Members' behalf—and, in doing so, entrusted American Vision with their PII/PHI while using its service; and (2) were required to provide their PII to American Vision in connection with their employment with the Ophthalmologist Defendants. Indeed, Plaintiffs were required to directly or indirectly entrust their PII/PHI to American Vision for Plaintiffs' own benefit in

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

order to receive medical services and American Vision was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

340. American Vision knew or should have known the risks of storing Plaintiffs' and all other Class Members's PII/PHI and the importance of maintaining secure systems. American Vision knew or should have known of the many data breaches that targeted healthcare providers—and their business associates—that collect and store PII/PHI in recent years.

341. Given the nature of American Vision's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, American Vision should have identified the vulnerabilities to its system and prevented the Data Breach from occurring.

342. American Vision breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to:

a. Exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII/PHI of Plaintiffs and Class Members;

b. Comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;

c. Comply with its own privacy policies;

d. Comply with regulations protecting the PII/PHI at issue during the period of the Data Breach;

e. Adequately monitor, evaluate, and ensure the security of American Vision's network and systems;

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

f. Recognize in a timely manner that PII/PHI had been compromised; and

g. Timely and adequately disclose the Data Breach.

343. Plaintiffs' and Class Members' PII/PHI would not have been compromised but for American Vision's wrongful and negligent breach of its duties.

344. American Vision's failure to take proper security measures to protect the sensitive PII/PHI of Plaintiffs and Class Members as described herein, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and copying of PII/PHI by unauthorized third parties. Given that healthcare providers and their business associates are prime targets for hackers, Plaintiffs and Class Members are part of a foreseeable, discernible group that was at high risk of having their PII/PHI misused or disclosed if not adequately protected by American Vision.

345. It was also foreseeable that American Vision's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiffs and Class Members.

346. As a direct and proximate result of American Vision's conduct, Plaintiffs and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT II

Negligence *Per Se*

(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses, Against American Vision)

347. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

348. As a healthcare provider business associate, American Vision is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

349. 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart C regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart D providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information," and Subpart E governing "Privacy of Individually Identifiable Health Information."

350. 45 C.F.R. § 164.104 states that the "standards, requirements, and implementation specifications adopted under this part" apply to covered entities and their business associates, such as American Vision.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

351. American Vision is obligated under HIPAA to, among other things, "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306.

352. 45 C.F.R. Sections 164.308 (Administrative safeguards), 164.310 (Physical safeguards), 164.312 (Technical safeguards), 164.314 (Organizational requirements), and 164.316 (Policies and procedures and documentation requirements) provide mandatory standards that all covered entities must adhere to.

353. American Vision violated HIPAA by failing to adhere to and meet the required standards as set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

354. Likewise, HIPAA regulations require covered entities "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach" to "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of" a data breach. 45 C.F.R. § 164.404. The notice must also contain a minimum amount of information regarding the breach (including the dates of the breach and its discovery), the types of protected health information that were involved, steps individuals should take to protect themselves from harm resulting from the breach, a description of what the entity is doing to investigate the breach and mitigate harm, and contact information to obtain further information. *Id.*

355. American Vision breached its notification obligations under HIPAA by failing to give timely and complete notice of the breach to Plaintiffs and Class Members.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

356. HIPAA requires American Vision to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

357. HIPAA further requires American Vision to disclose the unauthorized access and theft of the PHI to Plaintiffs and Class Members "without unreasonable delay" so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and detect misuse of their PHI. See 45 C.F.R. § 164.404.

358. American Vision violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' PHI and by failing to give timely and complete notice, as described herein.

359. American Vision's violations of HIPAA constitute negligence *per se*.

360. Plaintiffs and Class Members are within the class of persons that HIPAA and its implementing regulations were intended to protect.

361. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

362. Additionally, Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as American Vision, of failing to use reasonable measures to protect PII/PHI. 15 U.S.C. § 45(a)(1).

363. The FTC publications and orders described above also form part of the basis of American Vision's duty in this regard.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

364. American Vision violated Section 5 of the FTCA by failing to use reasonable measures to protect PII/PHI and failing to comply with applicable industry standards. American Vision's conduct was unreasonable given the nature and amount of PII/PHI it obtained, stored, and disseminated in the regular course of its business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiffs and Class Members.

365. American Vision's violations of Section 5 of the FTCA constitute negligence *per se*.

366. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

367. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was 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 and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

368. As a direct and proximate result of American Vision's conduct, Plaintiffs and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in American Vision's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses, Against American Vision)

369. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

370. Plaintiffs and Class Members conferred benefits on American Vision, both directly and indirectly, in the form of payments for medical and healthcare services and/or through labor. All Class Members also conferred a benefit upon American Vision in the form of their PII/PHI, which has inherent value and allowed American Vision to operate its business, collect payments from patients, and hire employees.

371. American Vision had knowledge of the benefits conferred by Plaintiffs and Class Members and appreciated, and retained, such benefits. In accepting PII/PHI, money, and labor from Plaintiffs and Class Members, whether directly or indirectly, American Vision should

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

have paid the costs of basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan.

372. In failing to provide such measures, American Vision has been unjustly enriched at Plaintiffs' and Class Members' expense. American Vision has no justification for failing to provide adequate security protections.

373. Plaintiffs and Class Members have suffered actual damages and harm because of American Vision's negligent, and unlawful, conduct, inactions, and omissions. American Vision should be required to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received from Plaintiffs and Class Members.

COUNT IV
Negligence
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses, Against Ophthalmologist Defendants)

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

374. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

375. Ophthalmologist Defendants owed a duty to Plaintiffs and Class Members, upon partnering with American Vision, to supervise and ensure American Vision maintained adequate data security for the protection of Plaintiffs' and Class Members' PII/PHI within its control for the purpose of carrying out the business of the partnership consistent with industry standards. Ophthalmologist Defendants owed nondelegable duty to exercise reasonable care in protecting Plaintiffs' and Class Members' PII/PHI from unauthorized disclosure or access. Ophthalmologist Defendants acknowledge this duty in their policies describing their handling of PII/PHI, where they promised not to disclose PII/PHI without authorization.

376. As healthcare providers, Ophthalmologist Defendants had a "special relationship" with Plaintiffs and Class Members who entrusted Ophthalmologist Defendants to adequately safeguard their PII/PHI. Indeed, because of that special relationship, and in order to receive medical services from Ophthalmologist Defendants, Plaintiffs provided Ophthalmologist Defendants with their private and valuable PII/PHI.

377. Ophthalmologist Defendants' duty to use reasonable care in protecting PII/PHI arises as a result of the parties' relationship, as well as common law, including Ophthalmologist Defendants' own policies and promises regarding privacy and data security.

378. Ophthalmologist Defendants knew or should have known the risks of collecting and storing Plaintiffs' and all other Class Members's PII/PHI and the importance of maintaining secure systems. Ophthalmologist Defendants knew or should have known of the many data breaches that targeted healthcare providers—and their business associates—that collect and store PII/PHI in recent years.

379. Given the nature of Ophthalmologist Defendants' business, the sensitivity and value of the PII/PHI it maintains and shares, and the resources at its disposal, Ophthalmologist Defendants should have identified the vulnerabilities to American Vision's systems and prevented the Data Breach from occurring.

380. Ophthalmologist Defendants breached these duties by failing to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members's PII/PHI by failing to, or contracting with companies that failed to:

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

a. Ensure their partner American Vision implemented security systems, protocols, and practices sufficient to protect the PII/PHI of Plaintiffs and Class Members;

b. Supervise their partner American Vision regarding its data security systems, protocols, and practices when it knew or should have known those systems, protocols, and practices were inadequate;

c. Comply with their own privacy policies;

d. Comply with regulations protecting the PII/PHI at issue during the period of the Data Breach;

e. Recognize in a timely manner that PII/PHI had been compromised; and

f. Timely and adequately disclose the Data Breach.

381. Plaintiffs' and Class Members' PII/PHI would not have been compromised but for Ophthalmologist Defendants' wrongful and negligent breach of its duties.

382. Ophthalmologist Defendants' failure to take proper security measures to protect the sensitive PII/PHI of Plaintiffs and Class Members as described herein, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and copying of PII/PHI by unauthorized third parties. Given that healthcare providers are prime targets for hackers, Plaintiffs and Class Members are part of a foreseeable, discernible group that was at high risk of having their PII/PHI misused or disclosed if not adequately protected by Ophthalmologist Defendants.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

383. It was also foreseeable that Ophthalmologist Defendants' failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiffs and Class Members.

384. As a direct and proximate result of Ophthalmologist Defendants' conduct, Plaintiffs and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Ophthalmologist Defendants' possession and is subject to further unauthorized disclosures so long as Ophthalmologist Defendants fail to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

COUNT V
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the State Subclasses, Against Ophthalmologist Defendants)

385. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

386. As healthcare providers, Ophthalmologist Defendants are covered by HIPAA, 45 C.F.R. § 160.102, and are therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

387. 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart C regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart D providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information," and Subpart E governing "Privacy of Individually Identifiable Health Information."

388. 45 C.F.R. § 164.104 states that the "standards, requirements, and implementation specifications adopted under this part" apply to covered entities and their business associates, such as Ophthalmologist Defendants.

389. Ophthalmologist Defendants are obligated under HIPAA to, among other things, "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306.

390. 45 C.F.R. Sections 164.308 (Administrative safeguards), 164.310 (Physical safeguards), 164.312 (Technical safeguards), 164.314 (Organizational requirements), and 164.316 (Policies and procedures and documentation requirements) provide mandatory standards that all covered entities must adhere to.

391. Ophthalmologist Defendants violated HIPAA by failing to adhere to and meet the required standards as set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

392. Likewise, HIPAA regulations require covered entities "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach" to "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of" a data breach. 45 C.F.R. § 164.404. The notice must also contain a minimum amount of information regarding the breach (including the dates of the breach and its discovery), the types of protected health information that were involved, steps individuals should take to protect themselves from harm resulting from the breach, a description of what the entity is doing to investigate the breach and mitigate harm, and contact information to obtain further information. *Id.*

393. Ophthalmologist Defendants breached their notification obligations under HIPAA by failing to give timely and complete notice of the breach to Plaintiffs and Class Members.

394. HIPAA requires Ophthalmologist Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

395. HIPAA further requires Ophthalmologist Defendants to disclose the unauthorized access and theft of the PHI to Plaintiffs and Class Members "without unreasonable delay" so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and detect misuse of their PHI. See 45 C.F.R. § 164.404.

396. Ophthalmologist Defendants violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' PHI and by failing to give timely and complete notice, as described herein.

397. Ophthalmologist Defendants' violations of HIPAA constitute negligence *per se*.

398. Plaintiffs and Class Members are within the class of persons that HIPAA and its implementing regulations were intended to protect.

399. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

400. Additionally, Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Ophthalmologist Defendants, of failing to use reasonable measures to protect PII/PHI. 15 U.S.C. § 45(a)(1).

401. The FTC publications and orders described above also form part of the basis of Ophthalmologist Defendants' duty in this regard.

402. Ophthalmologist Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect PII/PHI, failing to comply with applicable industry standards,

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

and failing to exercise appropriate managerial supervision over their partner American Vision, which is their right under the partnership, to ensure that American Vision maintained adequate data security measures to protect the PII/PHI of Plaintiffs and Class Members. Ophthalmologist Defendants' conduct was unreasonable given the nature and amount of PII/PHI it obtained, stored, and disseminated in the regular course of its business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiffs and Class Members.

403. Ophthalmologist Defendants' violations of Section 5 of the FTCA constitute negligence *per se*.

404. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

405. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was 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 and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

406. As a direct and proximate result of Ophthalmologist Defendants' conduct, Plaintiffs and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Ophthalmologist Defendants' possession and is subject to further unauthorized disclosures so long as Ophthalmologist Defendants fail to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

COUNT VI

Breach of Express Contract
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses, Against Ophthalmologist Defendants)

407. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

408. Ophthalmologist Defendants disseminated "Notices of Privacy Practices" to their patients which constitutes an agreement between Ophthalmologist Defendants and persons who provided their PHI to Ophthalmologist Defendants, including Plaintiffs and Class Members.

409. Plaintiffs and Class Members formed contracts with Ophthalmologist Defendants and complied with all obligations under such contracts when they provided PHI to Ophthalmologist Defendants subject to the Notices of Privacy Practices.

410. Ophthalmologist Defendants promised in the Notices of Privacy Practices that their patients "have the right to be notified if we or one of our Business Associates becomes aware of a breach of your unsecured PHI." Ophthalmologist Defendants also represented that they "may not disclose [patients'] PHI without [patients'] written authorization" outside of specific situations.

411. Ophthalmologist Defendants breached their agreements with Plaintiffs and Class Members when Ophthalmologist Defendants allowed for the disclosure of Plaintiffs' and Class Members' PHI without their authorization and in a manner that was inconsistent with the permissible authorizations set forth in the Notices of Privacy Practices, as well as when they failed to maintain the confidentiality of Plaintiffs' and Class Members' medical and treatment information.

412. As a direct and proximate result of Ophthalmologist Defendants' conduct, Plaintiffs and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Ophthalmologist Defendants' possession and is subject to further unauthorized

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

disclosures so long as Ophthalmologist Defendants fail to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded. Plaintiffs and Class Members did not receive the benefits of the bargains for which they paid.

COUNT VII
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses, Against Ophthalmologist Defendants)

413. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

414. Plaintiffs bring this cause of action in the alternative to their Breach of Express Contract claim above.

415. In connection with receipt of medical services and/or in connection as a condition of their employment, Plaintiffs and Class Members entrusted their PII/PHI to Ophthalmologist Defendants. In so doing, Plaintiffs and Class Members entered into implied contracts with Ophthalmologist Defendants by which Ophthalmologist Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

416. Implicit in the agreements between Plaintiffs, Class Members, and Ophthalmologist Defendants regarding the provision of PII/PHI, which Plaintiff and Class

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Members were required to provide to Defendant, were the following obligations for the Ophthalmologist Defendants: (a) restrict the use of such PII/PHI solely for business purposes, (b) implement reasonable measures to safeguard the PII/PHI, (c) prevent unauthorized disclosures of the PII/PHI, (d) promptly and adequately notify Plaintiff and Class Members of any unauthorized access and/or theft of their PII/PHI, (e) reasonably safeguard and protect the PII/PHI of Plaintiffs' and Class Members' from unauthorized disclosure or use, and (f) maintain the PII/PHI under conditions ensuring their security and confidentiality.

417. The mutual understanding and intent between Plaintiffs, Class Members, and Ophthalmologist Defendants are evident through their conduct and ongoing business interactions.

418. Plaintiffs and Class Members have an interest, both equitable and legal, in their PII/PHI that was conferred upon, collected by, and maintained by the Ophthalmologist Defendants and which was stolen in the Data Breach. This information has independent value.

419. Plaintiffs and Class Members conferred a benefit on Ophthalmologist Defendants in the form of payments for medical and healthcare services, including those paid indirectly by Plaintiffs and Class Members to Defendant, and/or labor.

420. Ophthalmologist Defendants appreciated and had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

421. As a direct and proximate result of Ophthalmologist Defendants' conduct, Plaintiffs and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Ophthalmologist Defendants' possession and is subject to further unauthorized disclosures so long as Ophthalmologist Defendants fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded. Plaintiffs and Class Members did not receive the benefits of the bargains for which they paid.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

COUNT VIII
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses, Against Ophthalmologist Defendants)

422. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

423. As healthcare providers and employees, Ophthalmologist Defendants had a confidential relationship with Plaintiffs and Class Members.

424. Plaintiffs and the Class Members maintained a confidential relationship with Ophthalmologist Defendants whereby Ophthalmologist Defendants assumed a duty to not

disclose the PII/PHI to unauthorized third parties. The PII/PHI was confidential, novel, highly personal, and sensitive.

425. Ophthalmologist Defendants knew Plaintiffs' and the Class Members' PII/PHI was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the PII/PHI they collected, stored, and maintained.

426. The Data Breach comprised unauthorized disclosure of Plaintiffs' and the Class Members' PII/PHI, in violation of this understanding. This non-consensual disclosure occurred because Ophthalmologist Defendants failed to exercise appropriate managerial control over American Vision's data security, which was their right as a partner in the partnership, when it knew American Vision was storing sensitive PII/PHI and when Ophthalmologist Defendants knew or should have known American Vision was unequipped to protect this information. Ophthalmologist Defendants' recklessness in failing to comply with industry-standard data security practices amounted to intentional behavior.

427. Plaintiffs and the Class Members suffered harm the moment the unauthorized disclosure of the PII/PHI to a third party occurred.

428. Plaintiffs and Class Members did not consent to nor authorize the release or disclosure of their PII/PHI to unknown third parties.

429. As a direct and proximate result of Ophthalmologist Defendants' conduct, Plaintiffs and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Ophthalmologist Defendants' possession and is subject to further unauthorized disclosures so long as Ophthalmologist Defendants fail to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

COUNT IX

Breach of Third-Party Beneficiary Contract

(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses, Against American Vision)

430. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

431. Acting in the ordinary course of business, American Vision entered into contracts with ophthalmologist practices to provide administrative and management services, which including storing Plaintiffs' and Class Members' PII/PHI received from those ophthalmologist practices.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

432. Upon information and belief, each of those respective contracts contained provisions requiring American Vision to protect the PII/PHI that it received in order to provide administrative and management services in carrying out the business of the partnership.

433. Upon information and belief, these provisions requiring American Vision acting in the ordinary course of business to protect the personal information of the third-party patients and employees was intentionally included for the direct benefit of Plaintiffs and Class Members, such that Plaintiffs and Class Members are intended third party beneficiaries of these contracts, and therefore entitled to enforce them.

434. American Vision breached these contracts while acting in the ordinary course of business by not protecting Plaintiffs' and Class Members' PII/ PHI , as stated herein.

435. As a direct and proximate result of American Vision's breaches, Plaintiffs and Class Members sustained actual losses and damages described in detail herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT X

Breach of Fiduciary Duty

(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses, Against Ophthalmologist Defendants)

436. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

437. A fiduciary relationship existed between Ophthalmologist Defendants and Plaintiffs and the Class Members. Plaintiffs and the Class Members placed Ophthalmologist Defendants in a position of trust and confidence by providing them with the PII/PHI as a

condition of their employment and/or receipt of medical services, which PII/PHI was accepted and appreciated by Ophthalmologist Defendants.

438. Ophthalmologist Defendants assumed a duty not to disclose the PII/PHI provided by Plaintiffs and the Class Members to unauthorized third parties. Again, the PII/PHI was confidential, novel, highly personal, and sensitive.

439. Ophthalmologist Defendants breached the fiduciary duty owed to Plaintiffs and the Class Members by failing to act with the utmost good faith, fairness, and honesty, and failing to protect the PII/PHI in its possession.

440. Plaintiffs and Class Members did not consent to nor authorize the release or disclosure of their PII/PHI to unknown third parties.

441. As a direct and proximate result of Ophthalmologist Defendants' conduct, Plaintiffs and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Ophthalmologist Defendants' possession and is subject to further unauthorized disclosures so long as Ophthalmologist Defendants fail to undertake appropriate and adequate

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT XI

Invasion of Privacy

(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

442. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

443. Plaintiffs and Class Members had a legitimate expectation of privacy in their PII/PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

444. Defendants owed a duty to Plaintiffs and Class Members, to keep their PII/PHI confidential.

445. Defendants failed to protect, and allowed unknown and unauthorized third parties to access, the PII/PHI of Plaintiffs and Class Members.

446. The PII/PHI that was publicized during the Data Breach was highly sensitive, private, and confidential.

447. Defendants acted with reckless disregard for the privacy of Plaintiffs and Class Members rising to the level of: (a) an intentional intrusion by Ophthalmologist Defendants; (b) into a matter that Plaintiffs and Class Members have a right to keep private (i.e., their PII/PHI); and (c) which is highly offensive to a reasonable person.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

448. American Vision acted knowingly when it failed to implement adequate safety measures to protect Plaintiffs' and Class Members' PII/PHI as explained above. Ophthalmologist Defendants acted knowingly when they permitted the Data Breach to occur; they had actual knowledge that their partner American Vision's information security practices were inadequate and insufficient.

449. Ophthalmologist Defendants were aware of the potential of a data breach and failed to exercise appropriate managerial control over American Vision's data security, which was their right as a partner in the partnership, when they knew American Vision was storing sensitive PII/PHI and when Ophthalmologist Defendants knew or should have known American Vision was unequipped to prevent the unauthorized release of Plaintiffs' and Class Members' data and PII/PHI.

450. Defendants acted with such reckless disregard as to the safety of Plaintiffs' and Class Members' PII/PHI to rise to the level of intentionally allowing the intrusion upon Plaintiffs' and Class Members' seclusion.

451. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII/PHI of Plaintiffs and Class Members would be highly offensive to a reasonable person.

452. Plaintiffs and Class Members did not consent to nor authorize the release or disclosure of their PII/PHI to unknown third parties.

453. Plaintiffs and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

COUNT XII

Unjust Enrichment

(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses, against the Ophthalmologist Defendants)

454. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

455. This Count is pleaded in the alternative to Plaintiffs' breach of express and implied contract claims above (Counts VI and VII).

456. Plaintiffs and Class Members conferred benefits on Ophthalmologist Defendants, both directly and indirectly, in the form of payments for payment for medical and healthcare services and/or through labor.

457. Ophthalmologist Defendants had knowledge of the benefits conferred by Plaintiffs and Class Members and appreciated, and retained, such benefits. In accepting PII/PHI, money, and labor from Plaintiffs and Class Members, Ophthalmologist Defendants should have paid the costs of basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan.

458. In failing to provide such measures, Ophthalmologist Defendants has been unjustly enriched at Plaintiffs' and Class Members' expense. Ophthalmologist Defendants have no justification for failing to provide adequate security protections.

459. Plaintiffs and Class Members have suffered actual damages and harm because of Defendant's negligent, and unlawful, conduct, inactions, and omissions. Ophthalmologist Defendants should be required to disgorge into a common fund for the benefit of Plaintiffs and

Class Members all unlawful or inequitable proceeds received from Plaintiffs and Class Members.

COUNT XIII

Violation of Arizona Consumer Fraud Act,
Ariz. Rev. Stat. § 44-152, *et seq.*
(On Behalf of Plaintiffs and the Arizona Class,
Against American Vision, Barnet, and SWEC)

460. Arizona Plaintiffs and the Arizona Class repeat and reallege every allegation set forth in the preceding paragraphs.

461. Arizona Plaintiffs the Arizona Class, and Defendant are "person[s]" under Ariz. Rev. Stat. § 44-1522(A).

462. The medical and healthcare services provided by Defendants are "merchandise" under Ariz. Rev. Stat. § 44-1522(A).

463. The Arizona Consumer Fraud Act ("ACFA") prohibits "[t]he act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby." Ariz. Rev. Stat. § 44-1522(A).

464. Defendants engaged in the intentional deceptive practices in connection with the sale and advertisement of their merchandise under Ariz. Rev. Stat. § 44-1522(A), including:

a. Representing that their services have characteristics, uses, and benefits that they do not have; and

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

b. Representing that their services are of a particular standard or quality if they are of another.

c. Misrepresenting that they maintained reasonable and adequate security measures;

d. Misrepresenting that they would comply with common law and statutory duties pertaining to security of their network, including duties imposed by Section 5 of the FTCA, HIPAA Privacy and Security Rules, and Ariz. Rev. Stat. § 18-*551 et seq*.;

e. Omitting, suppressing, and concealing the material fact that they did not exercise appropriate supervision over the data security measures of its partners with whom Defendants share Arizona Plaintiffs and the Arizona Class's PII/PHI; and

f. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security of their network, including duties imposed by Section 5 of the FTCA, HIPAA Privacy and Security Rules, and Ariz. Rev. Stat. § 18-*551 et seq*.

465. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security.

466. Defendants knowingly and willingly represented that their networks maintained adequate protections to induce Arizona Plaintiffs and the Arizona Class to use and rely on Defendants' services.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

467. Defendants' concealments, omissions, and false promises induced Arizona Plaintiffs and the Arizona Class to use and rely on Defendants' services. But for these unlawful acts by Defendants, Arizona Plaintiffs and the Arizona Class would not have used or relied on Defendants' services.

468. All Defendants separately engaged in unfair practices in connection with the sale and advertisement of merchandise under Ariz. Rev. Stat. § 44-1522(A), including:

a. Failing to control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols of its partners and business associates like American Vision;

b. Failing to comply with common law and statutory duties pertaining to the security of their network that houses Plaintiffs and the Arizona Class's PII/PHI, including duties imposed by Section 5 of the FTCA, HIPAA Privacy and Security Rules, and Ariz. Rev. Stat. § 18-551 *et seq.*;

c. Overcharging for services provided without adequate security measures in place.

469. As a direct and proximate result of Defendants' conduct, Arizona Plaintiffs and the Arizona Class have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT XIV

Violations of Texas Deceptive Trade Practices—Consumer Protection Act, Tex. Bus. & Com. Code §§ 17.41, *et seq*.
(On Behalf of Plaintiff Ralph Gallegos and the Texas Class, Against Defendant SWEI)

470. Plaintiff Ralph Gallegos and the Texas Class repeat and reallege every allegation set forth in the preceding paragraphs.

471. SWEI is a "person," as defined by Tex. Bus. & Com. Code Ann. § 17.45(3).

472. Plaintiff Gallegos and the Texas Class are "consumers," as defined by Tex. Bus. & Com. Code Ann. § 17.45(4).

473. SWEI advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code Ann. § 17.45(6).

474. SWEI engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code Ann. § 17.46(b), including:

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

a. Representing that services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that services are of a particular standard, quality or grade, if they are of another;

c. Advertising services with intent not to sell them as advertised; and

d. Failing to disclose information concerning services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

475. SWEI's false, misleading and deceptive acts and practices include:

a. Failing to control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols of its partners and business associates like American Vision, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, 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 Texas Plaintiff's and the Texas Class's PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

d. Misrepresenting that they would protect the privacy and confidentiality of Texas Plaintiff's and the Texas Class's PII/PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Texas Plaintiff's and the Texas Class's PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that SWEI did not exercise appropriate supervision over the data security measures of its partners with whom SWEI shared Texas Plaintiff's and the Texas Class's PII/PHI; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Texas Plaintiff's and the Texas Class's PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45.

476. SWEI intended to mislead Plaintiff Gallegos and the Texas Class and induce them to rely on its misrepresentation and omissions.

477. SWEI's representations and 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 consumers' PII/PHI.

478. Had SWEI disclosed to Plaintiff Gallegos and the Texas Class that it did not exercise appropriate managerial control over their business associates and partners whom SWEI

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

shared Texas Plaintiff's and the Texas Class's PII/PHI, SWEI would have been forced to adopt reasonable data security measures and comply with the law SWEI trusted with sensitive and valuable PII/PHI regarding millions of patients and employees, including Texas Plaintiff and the Texas Class. SWEI accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Texas Plaintiff and the Texas Class acted reasonably in relying on SWEI's misrepresentations and omissions, the truth of which it could not have discovered.

479. SWEI had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII/PHI in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between patients and employees, including Texas Plaintiff and the Texas Class, and SWEI because patients and employees are unable to fully protect their interests with regard to their data, and they placed trust and confidence in SWEI. SWEI's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Texas Plaintiff and the Texas Class that contradicted these representations.

480. SWEI engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). SWEI engaged in acts or practices which, to

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

patients' and employees' detriment, took advantage of their lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

481. Patients and employees, including Texas Plaintiff and the Texas Class, lacked knowledge about deficiencies in SWEI's data security because this information was known exclusively by SWEI. Patients and employees also lacked the ability, experience, or capacity to secure the PII/PHI in SWEI's possession or to fully protect their interests with regard to their data. Texas Plaintiff and the Texas Class lack expertise in information security matters and do not have access to SWEI's systems in order to evaluate its security controls. SWEI took advantage of its special skill and access to PII/PHI to hide its inability to protect the security and confidentiality of Texas Plaintiff's and the Texas Class's PII/PHI.

482. SWEI intended to take advantage of patients' and employees' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from SWEI's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from SWEI's unconscionable business acts and practices, exposed Texas Plaintiff and Texas Class to a wholly unwarranted risk to the safety of their PII/PHI and the security of their identity or credit and worked a substantial hardship on a significant and unprecedented number of individuals. Texas Plaintiff and Texas Class cannot mitigate this unfairness because they cannot undo the Data Breach.

483. SWEI acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Texas Plaintiff and the Texas Class's rights.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

484. As a direct and proximate result of SWEI's unconscionable and deceptive acts or practices, Texas Plaintiff and the Texas Class have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in SWEI's possession and is subject to further unauthorized disclosures so long as SWEI fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

485. SWEI's violations present a continuing risk to Texas Plaintiff and the Texas Class as well as to the general public.

486. Texas Plaintiff and the Texas Class seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

COUNT XV

Violations of Nevada Deceptive Trade Practices Act,
Nev. Rev. Stat. § 598.0903, *et seq*.
(On Behalf of Plaintiff Israel and the Nevada Class, Against Defendant Wellish)

487. Plaintiff Israel and the Nevada Class repeat and reallege every allegation set forth in the preceding paragraphs.

488. Plaintiff Israel brings this claim against Wellish.

489. Wellish advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada when it provided eyecare services in the state of Nevada.

490. Wellish knowingly engaged in a deceptive trade practice under N.R.S. § 598.01915 by: (a) Knowingly making a false representation as to the characteristics, uses, or benefits, in connection with the sale of a service; (b) Knowingly representing services of a particular standard, quality or grade despite knowing that they are of another standard, quality, grade, style or mode; (c) Knowingly representing that its services have approval, characteristics, uses, or benefits that they do not have; and (d) Knowingly advertising services with intent not to sell them as advertised.

491. Wellish's false, misleading and deceptive acts and practices include: (a) Failing to control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, which was a direct and proximate cause of the Data Breach; (b) Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, 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 Israel's and the Nevada Class's PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach; (d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Israel's and the Nevada Class's PII/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 Israel's and the Nevada Class's PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45; (f) Omitting, suppressing, and concealing the material fact that they did not exercise appropriate supervision over the data security measures of themselves and their partners with whom the Nevada Defendants shared Plaintiff Israel's and the Nevada Class's PII/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 Israel's and the Nevada Class's PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45.

492. Wellish intended to mislead Plaintiff Israel and the Nevada Class and induce them to rely on its misrepresentation and omissions.

493. Wellish's representations and 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 consumers' PII/PHI.

494. Wellish engaged in these deceptive acts knowingly because it knew or should have known its data security practices were not adequate. And Wellish knew, or should have known, that Plaintiff Israel and Nevada Class members had no means of discovering the inadequacy of Wellish's data security practices.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

495. Wellish had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII/PHI in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between patients and employees, including Plaintiff Israel and the Nevada Class, and Wellish, because patients and employees are unable to fully protect their interests with regard to their data, and they placed trust and confidence in Wellish. Wellish duty to disclose also arose from its: (a) Possession of exclusive knowledge regarding the security of the data in its systems; (b) Active concealment of the state of its security; and/or (c) Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Plaintiff Israel and the Nevada Class that contradicted these representations.

496. Wellish further engaged in unconscionable actions or courses of conduct, in violation of N.R.S. § 598.0923(1)(e) and (2)(b), by engaging in acts or practices which, to patients' and employees' detriment, took advantage of their lack of knowledge, ability, experience, or capacity to a grossly unfair degree. Specifically, Patients and employees, including Plaintiff Israel and the Nevada Class, lacked knowledge about deficiencies in Wellish's data security because this information was known exclusively by Wellish. Patients and employees also lacked the ability, experience, or capacity to secure the PII/PHI in Wellish's possession or to fully protect their interests with regard to their data. Plaintiff Israel and the Nevada Class lack expertise in information security matters and do not have access to Wellish's systems in order to evaluate its security controls. As such, the Nevada Defendants took advantage of their special skill and access to PII/PHI to hide their inability to protect the security and confidentiality of Plaintiff Israel's and the Nevada Class's PII/PHI.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

497. Wellish intended to take advantage of patients' and employees' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Wellish's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from Wellish's unconscionable business acts and practices, exposed Plaintiff Israel and Nevada Class to a wholly unwarranted risk to the safety of their PII/PHI and the security of their identity or credit and worked a substantial hardship on a significant and unprecedented number of individuals. Plaintiff Israel and Nevada Class cannot mitigate this unfairness because they cannot undo the Data Breach.

498. Wellish acted intentionally, knowingly, and maliciously to violate the Nevada Deceptive Trade Practices Act, and recklessly disregarded Plaintiff Israel and the Nevada Class's rights.

As a direct and proximate result of Wellish's unconscionable and deceptive acts or practices, Plaintiff Israel and the Nevada Class have and will suffer damages including: (i) the loss of rental or use value of their PII/PHI; (ii) the unconsented disclosure of their PII/PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

to their PII/PHI, which remains in Wellish's possession and is subject to further unauthorized disclosures so long as they fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

499. Wellish's violations present a continuing risk to Plaintiff Israel and the Nevada Class as well as to the general public.

500. Plaintiff Israel and the Nevada Class seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

COUNT XVI

Declaratory Judgment

(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

501. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Consolidated Complaint.

502. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard PII/PHI and whether Defendants are currently maintaining data security measures adequate to

protect Plaintiffs and Class Members from further cyberattacks and data breaches that could compromise their PII/PHI.

503. Defendants still possess PII/PHI pertaining to Plaintiffs and Class Members, which means their PII/PHI remains at risk of further breaches because Defendants' data security measures remain inadequate. Plaintiffs and Class Members continue to suffer injuries as a result of the compromise of their PHI and remain at an imminent risk that additional compromises of their PII/PHI will occur in the future.

504. Pursuant to the Declaratory Judgment Act, Plaintiffs seek a declaration that: (a) Defendants' existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Defendants must have policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii), (a)-(i), *infra*, and must comply with those policies and procedures; (2) Defendants must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiffs' and Class Members' PII/PHI if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

and violate the terms of the federal statutes described in this Consolidated Complaint.

b. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

c. Engaging third-party security auditors and internal personnel to run automated security monitoring;

d. Auditing, testing, and training its security personnel regarding any new or modified procedures;

e. Encrypting PII/PHI and segmenting PII/PHI by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of its systems;

f. Purging, deleting, and destroying in a reasonable and secure manner PII/PHI not necessary to perform essential business functions;

g. Conducting regular database scanning and security checks;

h. Conducting regular employee education regarding best security practices;

i. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

j. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiffs as class representatives and Plaintiffs' Interim Counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and Class Members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

F. That Plaintiffs be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiffs the costs and disbursements of the action, along

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

with reasonable attorneys' fees, costs, and expenses; and

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

Dated: August 1, 2024.

Respectfully submitted,

/s/ Cristina Perez Hesano
Cristina Perez Hesano (#027023)
cperez@perezlawgroup.com
PEREZ LAW GROUP, PLLC
7508 N. 59th Avenue
Glendale, AZ 85301
Telephone: 602.730.7100
Fax: 623.235.6173

Elaine A. Ryan (AZ Bar No. 012870)
Colleen M. Auer (AZ Bar No. 014637)
AUER RYAN, P.C.
20987 N. John Wayne Parkway, #B104-374
Maricopa, AZ 85139
(520) 705-7332
eryan@auer-ryan.com
cauer@auer-ryan.com

Interim Liaison Counsel

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Raina C. Borrelli
raina@ straussborrelli.com
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109

Terence R. Coates*
Jonathan T. Deters*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: 513.651.3700
Fax: 513.665.0219
tcoates@msdlegal.com
jdeters@msdlegal.com

Norman E. Siegel*
J. Austin Moore*
Stefon J. David*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
david@stuevesiegel.com

Interim Co-Lead Class Counsel
Amanda Boltax*
HAUSFELD LLP
888 16th Street, N.W., Suite 300
Washington, D.C. 20006
Telephone: (202) 540-7200
Facsimile: (202) 540-7201
aboltax@hausfeld.com

Patrick Donathen*
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel.: (412) 322-9243
patrick@lcllp.com

Nickolas J. Hagman
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Ste. 3210
Chicago, IL 60603
Phone: (312) 782-4880
nhagman@caffertyclobes.com

Cecily C. Jordan
cjordan@tousley.com
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Telephone: 206-682-5600
Facsimile: 206-682-2992

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut St., Ste 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com
Plaintiffs' Executive Committee Counsel

CERTIFICATE OF SERVICE

I hereby certify that on August 1, 2024, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the email addresses denoted on the Electronic Mail notice list.

*/s/ Cristina Perez Hesano*_____
Cristina Perez Hesano

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301