

**UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO**

Civil Action No. 1:24-cv-1694

THERESA OTERO, individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

PANORAMA EYE CARE, LLC,

Defendant.

COMPLAINT AND JURY DEMAND

CLASS ACTION COMPLAINT

Plaintiff Theresa Otero (“Plaintiff”), individually, and on behalf of all others similarly situated, bring this action against Panorama Eye Care, LLC (“Panorama” or “Defendant”). Plaintiff brings this action by and through her attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information and belief and reasonable investigation by her counsel as to all other matters, as follows.

I. INTRODUCTION

1. Panorama is a management services organization that serves eye care providers throughout Colorado and Wyoming. Panorama’s eye clinic clients include: Eye Center of Northern Colorado, Denver Eye Surgeons, Cheyenne Eye Clinic & Surgery Center, Boulder Eye Surgeons, Panorama Lasik, Haas Vision Center, Windsor Eye Care & Vision Center, Arvada Vision & Eye Clinic, 2020 Vision Center, and Evergreen Vision Clinic, PC.

2. As part of its operations, Panorama collects, maintains, and stores highly sensitive personal and medical information belonging to its clients’ patients, including, but not limited to

their full names, Social Security numbers, dates of birth, addresses, telephone numbers, driver's license numbers, military identification numbers, passport numbers (collectively, "personally identifying information" or "PII"), information regarding medical history, lab results, retina scans, prescriptions, medical treatments and diagnoses, medical record numbers, health insurance information, and other protected health information (collectively, "private health information" or "PHI"), bank account numbers, routing numbers, payment card numbers and expiration dates, and security/PIN numbers ("financial account information"), as well as usernames, passwords, email addresses, security questions and answers (collectively, with PII, PHI and financial account information, "Private Information").

3. According to Panorama's public statements, between May 22, 2023 and June 4, 2023, Panorama experienced a data breach incident in which unauthorized cybercriminals accessed its information systems and databases and stole Private Information belonging to Plaintiff and Class members (the "Data Breach"). Panorama discovered this unauthorized access on June 3, 2023. Panorama's subsequent investigation determined that the unauthorized actors were able to access and exfiltrate Private Information concerning Plaintiff and Class members.

4. On June 5, 2024, Panorama sent a notice to individuals whose information was accessed in the Data Breach.

5. Because Panorama stored and handled Plaintiff's and Class members' highly-sensitive Private Information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

6. Ultimately, Panorama failed to fulfill this obligation, as unauthorized cybercriminals breached Panorama's information systems and databases and stole vast quantities of Private Information belonging to Panorama's patients, including Plaintiff and Class members.

The Data Breach—and the successful exfiltration of Private Information—was the direct, proximate, and foreseeable results of multiple failings on the part of Panorama.

7. The Data Breach occurred because Panorama failed to implement reasonable security protections to safeguard its information systems and databases. Thereafter, Panorama failed to timely determine that the unauthorized cybercriminals accessed files containing the Private Information of Plaintiff and Class members until May 9, 2024, nearly *1 year* after the Data Breach. Moreover, before the Data Breach occurred, Panorama failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and Class members been made aware of this fact, they would have never provided such information to Panorama.

8. Panorama’s subsequent handling of the breach was also deficient.

9. Panorama’s failure to attempt to ameliorate the effects of the Data Breach with complimentary credit monitoring is woefully inadequate. Much of the Private Information that was stolen is immutable and identity theft protection and prevention (such as credit monitoring services) is paramount in the face of a life-long heightened risk of identity theft.

10. As a result of Panorama’s negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff and Class members suffered injuries, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;

- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in Panorama’s possession and is subject to further unauthorized disclosures so long as Panorama fails to undertake appropriate and adequate measures to protect their Private Information.

11. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief for the consequences of Panorama’s failure to reasonably safeguard Plaintiff’s and Class members’ Private Information; its failure to reasonably provide timely notification to Plaintiff and Class members that their Private Information had been compromised; and for Panorama’s failure to inform Plaintiff and Class members concerning the status, safety, location, access, and protection of their Private Information.

II. PARTIES

Plaintiff Theresa Otero

12. Plaintiff Otero is a resident and citizen of Fort Upton, Colorado. Plaintiff Otero’s minor daughter, Mysteek Pruet, is a patient at Panorama. Plaintiff Otero received Panorama’s Data Breach Notice.

Panorama Eye Care, LLC

13. Defendant Panorama is a Delaware corporation with its principal place of business located at 2809 E. Harmony Rd., Suite 210, Fort Collins, CO 80525. Panorama conducts business in this District and throughout the State of Colorado.

III. JURISDICTION AND VENUE

14. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in

controversy exceeds the sum of \$5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Panorama. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

15. This Court has personal jurisdiction over Panorama because Panorama is headquartered in this District.

16. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District and because Panorama resides in this District.

IV. FACTUAL ALLEGATIONS

A. Panorama – Background

17. Panorama is a management services organization that serves eye care providers throughout Colorado and Wyoming. Panorama's eye clinic clients include: Eye Center of Northern Colorado, Denver Eye Surgeons, Cheyenne Eye Clinic & Surgery Center, Boulder Eye Surgeons, Panorama Lasik, Haas Vision Center, Windsor Eye Care & Vision Center, Arvada Vision & Eye Clinic, 2020 Vision Center, and Evergreen Vision Clinic, PC. As part of its normal operations, Panorama collects, maintains, and stores large volumes of Private Information belonging to its current and former patients.

18. Panorama failed to implement necessary data security safeguards at the time of the Data Breach. This failure resulted in cybercriminals accessing the Private Information of Panorama's current and former patients—Plaintiff and Class members.

19. Current and former patients of Panorama, such as Plaintiff and Class members, made their Private Information available to Panorama with the reasonable expectation that any

entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

20. This expectation was objectively reasonable and based on an obligation imposed on Panorama by statute, regulations, industrial custom, and standards of general due care.

21. Unfortunately for Plaintiff and Class members, Panorama failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it failed to protect Plaintiff and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

22. According to Panorama's public statements, cybercriminals breached Panorama's information systems between May 22, 2023 and June 4, 2023. During that time, cybercriminals accessed and stole Private Information belonging to Plaintiff and Class members. Panorama discovered this unauthorized access on June 3, 2023, meaning that the criminals had access to Panorama's systems for a day after Panorama discovered the unauthorized access. Panorama conducted a subsequent investigation, and on May 9, 2024, determined that the unauthorized actors were able to access and exfiltrate Private Information concerning Plaintiff and Class members.

23. On June 5, 2024, Panorama sent notice of the Data Breach to all individuals affected by this data security incident.

24. Panorama estimates that the Private Information belonging to at least 377,911 individuals was compromised in this incident.

C. Panorama's Many Failures Both Prior to and Following the Breach

25. Panorama collects and maintains vast quantities of Private Information belonging to Plaintiff and Class members as part of its normal operations. The Data Breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Panorama.

26. Panorama inexcusably failed to implement reasonable security protections to safeguard its information systems and databases.

27. Panorama failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and Class members been aware that Panorama did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Panorama.

28. In addition to the failures that lead to the successful breach, Panorama's failings in handling the breach and responding to the incident exacerbated the resulting harm to the Plaintiff and Class members.

29. Panorama's delay in informing victims of the Data Breach that their Private Information was compromised virtually ensured that the cybercriminals who stole this Private Information could monetize, misuse and/or disseminate that Private Information before the Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

30. Additionally, Panorama's attempt to ameliorate the effects of the Data Breach with any credit monitoring for victims is inexcusable. Plaintiff's and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. Indeed, misusing highly sensitive Private Information, such as committing identity theft or

selling the Private Information on the dark web for others to use for identity theft, is the *modus operandi* of cybercriminals. As a consequence, Plaintiffs and Class members face a real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information, such as healthcare data, is immutable.

31. In short, Panorama's myriad failures, including the failure to timely detect an intrusion and failure to timely notify Plaintiff and Class members that their personal, medical and financial information had been stolen due to Panorama's security failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiff's and Class members' Private Information for over *one year* before Panorama finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

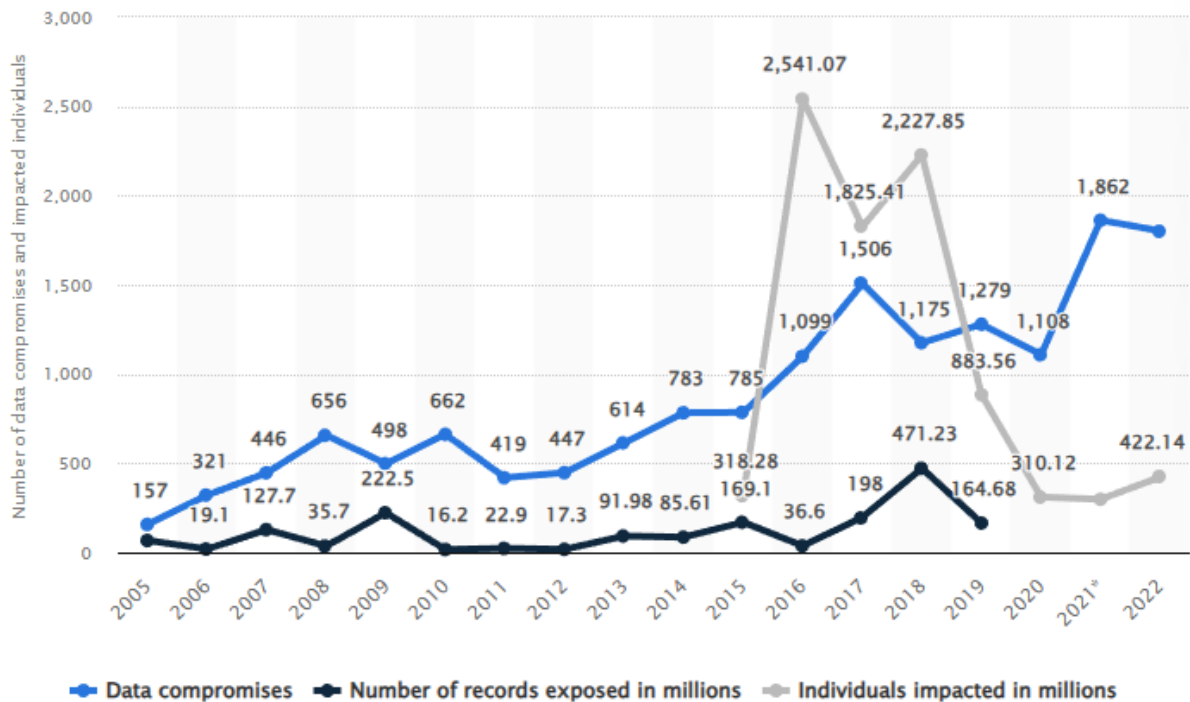
32. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, and Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

33. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.¹ The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just 8 shy of the

¹ *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report.

record of 715 set in 2021 and still double that of the number of similar such compromises in 2017 and triple the number of compromises in 2012.²

34. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.³ The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.⁴



² 2022 Healthcare Data Breach Report, The HIPAA Journal (January 24, 2023), available at: <https://www.hipaajournal.com/2022-healthcare-data-breach-report/>.

³ Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022, Statista, available at: <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>.

⁴ *Id.*

35. This stolen PII is then routinely traded on dark web black markets as a simple commodity, with social security numbers being so ubiquitous to be sold at as little as \$2.99 apiece and passports retailing for as little as \$15 apiece.⁵

36. In addition, the severity of the consequences of a compromised social security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory groups can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

[a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.⁶

This is exacerbated by the fact that the problems arising from a compromised social security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.⁷

⁵ *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: <https://cybernews.com/security/whats-your-identity-worth-on-dark-web/>.

⁶ United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

⁷ *Id.*

37. The most sought after and expensive information on the dark web are stolen medical records which command prices from \$250 to \$1,000 each.⁸ Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and social security numbers, which can be changed, medical records contain “a treasure trove of unalterable data points, such as a patient’s medical and behavioral health history and demographics, as well as their health insurance and contact information.”⁹ With this bounty of ill-gotten information, cybercriminals can steal victims’ public and insurance benefits and bill medical charges to victims’ accounts.¹⁰ Cybercriminals can also change the victims’ medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.¹¹ Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.¹²

38. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of \$13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer’s liability for fraudulent medical debt (in contrast, a consumer’s

⁸ Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (January 26, 2021), available at: <https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web>.

⁹ *Id.*

¹⁰ *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), available at <https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare>. See also Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (August 25, 2016), available at <https://www.consumerreports.org/health/medical-identity-theft-a1699327549/>.

¹¹ *Id.*

¹² *Id.*

liability for fraudulent credit card charges is capped at \$50).¹³ It is also “considerably harder” to reverse the damage from the aforementioned consequences of medical identity theft.¹⁴

39. Instances of Medical identity theft have grown exponentially over the years from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.¹⁵

40. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Panorama charged with maintaining and securing patient Private Information should know the importance of protecting that information from unauthorized disclosure. Indeed, Panorama knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.¹⁶

41. In addition, the Federal Trade Commission (“FTC”) has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers’ personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Panorama on notice of their obligation to safeguard customer and patient information.¹⁷

¹³ Medical Identity Theft, AARP (March 25, 2022), available at: <https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html>.

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ See, e.g., *Healthcare Data Breach Statistics*, HIPAA Journal, available at: <https://www.hipaajournal.com/healthcare-data-breach-statistics>.

¹⁷ See, e.g., *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).

42. Given the nature of Panorama’s Data Breach, as well as the length of the time Panorama’s networks were breached and the long delay in notification to victims thereof, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff’s and Class members’ Private Information can easily obtain Plaintiff’s and Class members’ tax returns or open fraudulent credit card accounts in their names.

43. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.¹⁸ The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

44. To date, Panorama has offered its consumers only limited identity theft monitoring services. The services offered are inadequate to protect Plaintiff and Class members from the threats they will face for years to come, particularly in light of the Private Information at issue here.

45. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, Panorama failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from misappropriation. As a result, the injuries to Plaintiff and Class members were directly and

¹⁸ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>. See also *Why Your Social Security Number Isn’t as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at <https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/>.

proximately caused by Panorama’s failure to implement or maintain adequate data security measures for its current and former patients.

E. Panorama Had a Duty and Obligation to Protect Private Information

46. Panorama has an obligation to protect the Private Information belonging to Plaintiff and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and medical records. Third, Panorama imposed such an obligation on itself with its promises regarding the safe handling of data. Plaintiff and Class members provided, and Panorama obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. HIPAA Requirements and Violation

47. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

48. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, “unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . . .” 45 CFR § 164.402.

49. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires entities to provide notice of a data breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach*” (emphasis added).

50. Panorama failed to implement and/or maintain procedures, systems, and safeguards to protect the Private Information belonging to Plaintiff and Class members from unauthorized access and disclosure.

51. Upon information and belief, Panorama’s security failures include, but are not limited to:

- a. Failing to maintain an adequate data security system to prevent data loss;
- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality and integrity of electronic protected health information Panorama creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);
- d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);
- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);
- f. Failing to identify and respond to suspected or known security incidents;
- g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);
- h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);
- i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

- j. Failing to ensure compliance with HIPAA security standard rules by Panorama’s workforce, in violation of 45 CFR 164.306(a)(94); and
- k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

52. Upon information and belief, Panorama also failed to store the information it collected in a manner that rendered it, “unusable, unreadable, or indecipherable to unauthorized persons,” in violation of 45 CFR § 164.402.

53. Panorama also violated the HIPAA Breach Notification Rule since it did not inform Plaintiff and Class members about the breach until 381 days after it first discovered the breach.

2. FTC Act Requirements and Violations

54. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

55. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.¹⁹ The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt

¹⁹ *Protecting Personal Information: A Guide for Business*, Federal Trade Comm’n (Oct. 2016), available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.²⁰ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²¹ Panorama clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

56. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

59. As evidenced by the Data Breach, Panorama failed to properly implement basic data security practices. Panorama's failure to employ reasonable and appropriate measures to

²⁰ *Id.*

²¹ *Id.*

protect against unauthorized access to Plaintiff's and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

60. Panorama was fully aware of its obligation to protect the Private Information of its current and former patients, including Plaintiff and Class members. Panorama is a sophisticated and technologically savvy business that relies extensively on technology systems and networks to maintain its practice, including storing its patients' Private Information in order to operate its business.

61. Panorama had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Panorama and Plaintiff and Class members. Panorama alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' Private Information.

3. Industry Standards and Noncompliance

62. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

63. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information, like Panorama, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Panorama failed to follow some or all of these industry best practices.

64. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Panorama failed to follow these cybersecurity best practices.

65. Panorama should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

66. Panorama failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

4. Panorama's Own Stated Policies and Promises

67. Panorama's own published privacy policy states that: "Panorama Eyecare honors the privacy of patients' and Associates' personal medical and non-medical information just as we expect our privacy to be protected." "Panorama Eyecare is committed to preserving patient's protected health information. Protected health information includes health information, diagnosis, treatments, personal data, billing and contact information."

68. Panorama failed to live up to its own stated policies and promises with regards to data privacy and data security as cybercriminals were able to infiltrate its systems and steal the Private Information belonging to Plaintiff and Class members.

F. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

69. Like any data hack, the Data Breach presents major problems for all affected.²²

70. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, “once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance.”²³

71. The ramifications of Panorama’s failure to properly secure Plaintiff’s and Class members’ Private Information are severe. Identity theft occurs when someone uses another person’s financial, and personal information, such as that person’s name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

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

73. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

74. Accordingly, Panorama’s wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal *Preventive Medicine Reports*, public and corporate data breaches correlate to an

²² Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at <https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers>.

²³ *Warning Signs of Identity Theft*, Federal Trade Comm’n, available at <https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft>.

increased risk of identity theft for victimized consumers.²⁴ The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.²⁵

75. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

76. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being \$4.45 million dollars in 2023.²⁶ The average cost to resolve a data breach involving health information, however, is more than double this figure at \$10.92 million.²⁷

77. The theft of medical information, beyond the theft of more traditional forms of PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far outstrips the increase in incidence of traditional identity theft.²⁸ Medical Identity Theft is especially nasty for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at \$50),

²⁴ David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at <https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub>.

²⁵ *Id.*

²⁶ *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRINbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclidsrc=aw.ds.

²⁷ *Id.*

²⁸ Medical Identity Theft, AARP (March 25, 2022), available at: <https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html>.

the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, \$13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.²⁹

78. In response to the Data Breach, Panorama failed to offer to provide certain individuals whose Private Information was exposed in the Data Breach with complimentary credit monitoring. This is inadequate to protect victims of the Data Breach from the lifelong risk of harm imposed on them by Panorama's failures.

79. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

- a. Theft of Private Information;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;
- c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;
- d. Costs associated with time spent to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Panorama's delay in disseminating notice in accordance with state law;
- e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

²⁹ *Id.*

f. The loss of Plaintiff's and Class members' privacy.

80. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will not abate within the limited time of credit monitoring offered by Panorama.

81. As a direct and proximate result of Panorama's acts and omissions in failing to protect and secure Private Information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and they have incurred and will incur actual damages in an attempt to prevent identity theft.

82. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

G. EXPERIENCES SPECIFIC TO PLAINTIFF

Plaintiff Otero

83. Plaintiff Otero's minor daughter, Mysteek Pruett, is a current patient of Panorama.

84. Plaintiff Otero received Panorama's Data Breach notice. The notice informed Plaintiff Otero that her minor daughter's Private Information was improperly accessed and obtained by third parties, including but not limited to Plaintiff's daughter's full name, telephone number, date of birth, medical history, prescription information, treating/referring physician name, medical record number (MRN), medical treatment information, medical diagnosis information, and Medicare or Medicaid number.

85. As a result of the Data Breach, Plaintiff has 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 Otero has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

86. After the Data Breach, Plaintiff Otero noticed a dramatic increase in the number of spam phone calls and emails and also was forced to replace her debit card three times this year due to frequent fraudulent activity and charges.

87. As a result of the Data Breach, Plaintiff Otero has suffered anxiety due to the public dissemination of her minor daughter's personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

88. Plaintiff Otero suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her minor daughter's Private Information, a form of property that Panorama obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

89. As a result of the Data Breach, Plaintiff Otero anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, both her and her minor daughter are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS REPRESENTATION ALLEGATIONS

90. Plaintiff brings this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are Panorama, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

91. In the alternative, Plaintiff brings this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

All persons who are residents of the State of Colorado whose Private Information was accessed in the Data Breach (the “Colorado Subclass”).

Excluded from the Subclass are Panorama, its executives and officers, and the Judge(s) assigned to this case.

92. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Panorama and obtainable by Plaintiff only through the discovery process. On information and belief, the number of affected individuals estimated to be 377,911.³⁰ The members of the Class will be identifiable through information and records in Panorama’s possession, custody, and control.

93. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over

³⁰ <https://apps.web.maine.gov/online/aeviewer/ME/40/a6b8d97b-71cf-417b-9585-bdbc8251b836.shtml> (last accessed June 14, 2024).

the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

- a. When Panorama learned of the Data Breach;
- b. Whether hackers obtained Class members' Private Information via the Data Breach;
- c. Whether Panorama's response to the Data Breach was adequate;
- d. Whether Panorama failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- e. Whether Panorama knew or should have known that its data security systems and monitoring processes were deficient;
- f. Whether Panorama owed a duty to safeguard their Private Information;
- g. Whether Panorama breached its duty to safeguard Private Information;
- h. Whether Panorama had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;
- i. Whether Panorama breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;
- j. Whether Panorama's conduct violated the FTCA, HIPAA, and/or the Consumer Protection Act invoked herein;
- k. Whether Panorama's conduct was negligent;
- l. Whether Panorama's conduct was *per se* negligent;
- m. Whether Panorama was unjustly enriched;
- n. What damages Plaintiff and Class members suffered as a result of Panorama's misconduct;
- o. Whether Plaintiff and Class members are entitled to actual and/or statutory damages; and
- p. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief.

94. Typicality: Plaintiff's claims are typical of the claims of the Class as Plaintiff and all members of the Class had their Private Information compromised in the Data Breach. Plaintiff's claims and damages are also typical of the Class because they resulted from Panorama's uniform wrongful conduct. Likewise, the relief to which Plaintiff is entitled to is typical of the Class because Panorama has acted, and refused to act, on grounds generally applicable to the Class.

95. Adequacy: Plaintiff is an adequate class representatives because Plaintiff's interests do not materially or irreconcilably conflict with the interests of the Class Plaintiff seeks to represent, Plaintiff has retained counsel competent and highly experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor Plaintiff's counsel have any interests that are antagonistic to the interests of other members of the Class.

96. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class, a class action is superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Panorama's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Panorama's records and databases.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE

(By Plaintiff on behalf of the Class)

97. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

98. Panorama owes a duty of care to protect the Private Information belonging to Plaintiff and Class members. Panorama also owes several specific duties including, but not limited to, the duty:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. to protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
- c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;
- d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class members pursuant to the FTCA;
- e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- f. to promptly notify Plaintiff and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

99. Panorama owes this duty because it had a special relationship with Plaintiff's and Class members. Plaintiff and Class members entrusted their Private Information to Panorama on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only Panorama had the ability to protect its systems and the Private Information stored on them from attack.

100. Panorama also owes this duty because industry standards mandate that Panorama protect its patients' confidential Private Information.

101. Panorama also owes a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiff and Class members. This duty exists to provide Plaintiff and Class members with the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

102. Panorama breached its duties owed to Plaintiff and Class members by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard their Private Information.

103. Panorama also breached the duties it owed to Plaintiff and Class members by failing to timely and accurately disclose to them that their Private Information had been improperly acquired and/or accessed.

104. As a direct and proximate result of Panorama's conduct, Plaintiff and Class members were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; and
- Permanent increased risk of identity theft.

105. Plaintiff and Class members were foreseeable victims of any inadequate security practices on the part of Panorama and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

106. In failing to provide prompt and adequate individual notice of the Data Breach, Panorama also acted with reckless disregard for the rights of Plaintiff and Class members.

107. Plaintiff and the Class are entitled to damages in an amount to be proven at trial and injunctive relief requiring Panorama to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT II
NEGLIGENCE PER SE
(By Plaintiff on behalf of the Class)

108. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

109. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, imposes a duty on Panorama to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiff and Class members.

110. HIPAA imposes a duty on Panorama to implement reasonable safeguards to protect Plaintiff's and Class members' Private Information. 42 U.S.C. § 1302(d), *et seq.*

111. HIPAA also requires Panorama to render unusable, unreadable, or indecipherable all Private Information it collected. Panorama was required to do so through “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.” *See* definition of “encryption” at 45 C.F.R. § 164.304.

112. In the event of a data breach, HIPAA obligates Covered Entities and Business Associates to notify affected individuals, prominent media outlets, and the Secretary of the Department of Health and Human Services of the data breach without unreasonable delay and in no event later than 60 days after discovery of the data breach. 45 CFR § 164.400, *et seq.*

113. Panorama violated the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiff's and Class members' Private Information.

114. Panorama violated HIPAA by failing to properly encrypt the Private Information it collected.

115. Panorama violated HIPAA by unduly delaying reasonable notice of the actual breach; in this case by 381 days.

116. Panorama's failure to comply with HIPAA and the FTCA constitutes negligence *per se*.

117. Plaintiff and Class members are within the class of persons that the FTCA and HIPAA are intended to protect.

118. It was reasonably foreseeable that the failure to protect and secure Plaintiff's and Class members' Private Information in compliance with applicable laws and industry standards would result in that Information being accessed and stolen by unauthorized actors.

119. As a direct and proximate result of Panorama's negligence *per se*, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

120. Plaintiff and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Panorama to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT III
UNJUST ENRICHMENT
(By Plaintiff on behalf of the Class)

121. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

122. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Panorama.

123. Panorama was benefitted by the conferral of Plaintiff's and Class members' Private Information and by its ability to retain and use that information. Panorama understood that it was in fact so benefitted.

124. Panorama also understood and appreciated that Plaintiff's and Class members' Private Information was private and confidential and its value depended upon Panorama maintaining the privacy and confidentiality of that information.

125. But for Panorama's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provided or authorized their Private Information to be provided to Panorama, and Panorama would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining patients, gaining the reputational advantages conferred upon it by Plaintiff and Class members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

126. As a result of Panorama's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiff, the Class, and the public relating to the nature and scope of

the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiff and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information), Panorama has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

127. Panorama's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

128. Under the common law doctrine of unjust enrichment, it is inequitable for Panorama to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and Class members in an unfair and unconscionable manner.

129. The benefit conferred upon, received, and enjoyed by Panorama was not conferred officiously or gratuitously, and it would be inequitable and unjust for Panorama to retain the benefit.

130. Panorama is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Panorama as a result of its wrongful conduct, including specifically the value to Panorama of the PII and medical information that was accessed and exfiltrated in the Data Breach and the profits Panorama receives from the use and sale of that information.

131. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Panorama and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Panorama from its wrongful conduct.

132. Plaintiff and Class members may not have an adequate remedy at law against Panorama, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
INVASION OF PRIVACY
(By Plaintiff on behalf of the Class)

133. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

134. Plaintiff and Class members had a reasonable expectation of privacy in the Private Information that Panorama possessed and/or continues to possess.

135. By failing to keep Plaintiff's and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Panorama invaded Plaintiff's and Class members' privacy by:

- a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and
- b. Publicizing private facts about Plaintiff and Class members, which is highly offensive to a reasonable person.

136. Panorama knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider Panorama's actions highly offensive.

137. Panorama invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

138. As a proximate result of such misuse and disclosures, Plaintiff's and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Panorama's conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

139. In failing to protect Plaintiff's and Class members' Private Information, and in misusing and/or disclosing their Private Information, Panorama has acted with malice and oppression and in conscious disregard of Plaintiff's and Class members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its millions of patients. Plaintiff, therefore, seeks an award of damages, including punitive damages, individually and on behalf of the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in their favor and against Panorama, as follows:

- A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;
- B. That Plaintiff be granted the declaratory relief sought herein;
- C. That the Court grant permanent injunctive relief to prohibit Panorama from continuing to engage in the unlawful acts, omissions, and practices described herein;
- D. That the Court award Plaintiff and Class members compensatory, consequential, and general damages in an amount to be determined at trial;
- E. That the Court award Plaintiff and Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;
- F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
- G. That the Court award pre- and post-judgment interest at the maximum legal rate;
- H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and
- I. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the putative Class, demands a trial by jury on all issues so triable.

Date: June 17, 2024

Respectfully Submitted,

/s/ Kathryn Stimson

Kathryn Stimson, #36783
Stimson, LaBranche, Hubbard, LLC
1652 N. Downing St
Denver, CO 80218
stimson@slhlegal.com

Daniel O. Herrera
Nickolas J. Hagman
**CAFFERTY CLOBES MERIWETHER
& SPRENGEL LLP**
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Negligent Cybersecurity to Blame for Panorama Eyecare Data Breach Affecting 377K Patients, Class Action Claims](#)
