

**UNITED STATES DISTRICT COURT  
DISTRICT OF COLORADO**

---

SARAH JONES, individually and on behalf  
of all others similarly situated,

Plaintiff,

v.

PANORAMA EYE CARE, LLC,

Defendant.

---

Case No.

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Sarah Jones, on behalf of herself and all others similarly situated (“Class Members,” as defined *infra*), alleges the following against Defendant Panorama Eye Care, LLC (“Defendant”) based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents, as to all other matters:

**INTRODUCTION**

1. Defendant is an eye care management company based in Fort Collins, Colorado that serves eye care providers throughout Colorado and Wyoming.

2. As a part of providing those services, Defendant acquired and maintained the personally identifiable information (“PII”) and protected health information (“PHI”) (collectively, “Private Information”) of consumers, including Plaintiff.

3. On June 3, 2023, Defendant discovered it had lost control over its computer network and the highly sensitive personal information stored on its computer network in a data breach perpetrated by cybercriminals (“Data Breach”). Upon information and belief, the Data Breach’s impact has been substantial, affecting nearly 378,000 individuals.

4. On information and belief, the Data Breach took place from May 22, 2023, to June

4, 2023. Following an investigation that concluded on or about May 9, 2024, Defendant learned cybercriminals had gained unauthorized access to consumer’s Private Information, including but not limited names, Social Security numbers, dates of birth, driver’s license numbers/state IDs, financial account information, dates of service, and medical provider names.<sup>1</sup>

5. On or about June 5, 2024—more than a year after the Data Breach occurred—Defendant finally began notifying Class Members about the Data Breach (“Notice Letter”).

6. Upon information and belief, cybercriminals were able to breach Defendant’s systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the Private Information of Plaintiffs, and failed to maintain reasonable security safeguards or protocols to protect Plaintiff’s and Class Member’s Private Information—rendering them easy targets for cybercriminals.

7. Defendant’s Notice Letter obfuscated the nature of the breach and the threat it posed—refusing to tell victims how many people were impacted, how the breach happened, when it discovered the breach, or why it took Defendant nine months to finally begin notifying victims that cybercriminals had gained access to their highly private information.

8. Defendant’s failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Private Information.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of Private Information misuse.

---

<sup>1</sup> <https://www.hipaajournal.com/panorama-eyecare-notifies-377k-individuals-a-year-after-ransomware-attack/>.

10. Plaintiff and Class Members are victims of Defendant’s negligence and inadequate cyber security measures. Specifically, Plaintiff and Class Members trusted Defendant with their Private Information. However, Defendant betrayed that trust by failing to properly use up-to-date security practices to prevent the Data Breach.

11. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys’ fees, the calculation of which will be based on information in Defendant’s possession.

12. The exposure of one’s Private Information to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the Private Information of Plaintiff and Class Members was exactly that—private. No longer. Now, their Private Information is permanently exposed and unsecure, leaving them at a heightened and imminent risk of fraud and identity theft.

### **PARTIES**

13. Plaintiff is a natural person and citizen of Colorado, residing in Fort Collins, Colorado. Plaintiff’s Notice Letter is attached as *Exhibit A*.

14. Defendant is a Delaware limited liability company with its principal place of business located at 2809 E. Harmony Road, Suite 210, Fort Collins, Colorado 80525. Upon information and belief, its members are citizens of states other than at least one Class Member.

### **JURISDICTION & VENUE**

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. There are over 100 putative Class Members, and at least one Class Member is a citizen of a state different from Defendant.

16. This Court has personal jurisdiction over Defendant because it is headquartered in

this District.

17. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

## **FACTUAL ALLEGATIONS**

### ***Defendant's Business***

18. Defendant is a management services organization that serves eye care providers throughout Colorado and Wyoming. Defendant'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. It boasts \$73.4 Million in annual revenue.

19. While administering services, Defendant accumulates the Private Information of consumers.

20. As a sophisticated management services organization serving eye care providers, with an acute interest in maintaining the confidentiality of the Private Information entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding the Private Information in its possession.

21. Consequently, Defendant agreed it would safeguard the data in accordance with its internal policies as well as state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Private Information.

22. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect consumer Private Information or trained its IT or data security employees to prevent, detect, and stop breaches of its

systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' Private Information.

***The Data Breach***

23. On information and belief, Defendant collects and maintains consumers' unencrypted Private Information in its computer systems.

24. In collecting and maintaining Private Information, Defendant implicitly agreed that it will safeguard the data using reasonable means according to their internal policies as well as state and federal law.

25. On or about June 5, 2024, Defendant sent Class Members a Notice Letter, notifying them of Data Breach that occurred in May 2023.

26. LockBit ransomware added Defendant its leak site in July 2023, claiming to have exfiltrated 798 GB of data from the company.<sup>2</sup> LockBit claims to have obtained data from Defendant's clients, including Eye Center of Northern Colorado, Denver Eye Surgeons, Cheyenne Eye Clinic & Surgery Center, and 2020 Vision Center.<sup>3</sup>

27. Defendant did not mention LockBit in its Notice Letter, which states, in part:

*What Happened?*

On or about June 3, 2024, Panorama learned that an unauthorized party may have obtained access to Panorama's internal network.

*What We Are Doing.*

Upon learning of this issue, we immediately secured the environment and commenced a prompt and thorough investigation. After a thorough and detailed forensic investigation, we determined the unauthorized actor access our network between May 22, 2023 and June 4, 2023, and, as a result may have accessed and removed certain files from our network

---

<sup>2</sup> See <https://healthitsecurity.com/news/eye-care-company-suffers-377k-record-data-breach>; see also <https://www.hipaajournal.com/panorama-eyecare-notifies-377k-individuals-a-year-after-ransomware-attack/>.

<sup>3</sup> <https://www.hipaajournal.com/panorama-eyecare-notifies-377k-individuals-a-year-after-ransomware-attack/>.

and environment. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents to conduct a comprehensive review of the impacted files and on May 9, 2024, we discovered that certain impacted files containing personal information may have been access and/or acquired by an unauthorized individual.

*What Information Was Involved?*

The impacted information includes your full name and, address, telephone number, date of birth, medical history, prescription information, treating/referring physician name, patient number, medical treatment information, [and] medical diagnosis information.<sup>4</sup>

28. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

29. Defendant’s “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

30. Through its inadequate security practices, Defendant exposed Plaintiff’s’ and Class Member’s Private Information for theft and sale on the dark web.

31. Despite its duties to safeguard Private Information, Defendant did not in fact follow industry standard practices in securing consumers’ Private Information, as evidenced by the Data Breach.

32. In response to the Data Breach, Defendant contends that it “immediately secured the environment and commenced a prompt and thorough investigation.”<sup>5</sup> Although Defendant fails

---

<sup>4</sup> *See, e.g.*, Ex. A.

<sup>5</sup> *Id.*

to expand on what how it “secured the environment,” such actions should have done before the Data Breach.

33. Through its Notice Letter, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims “to plac[e] a Fraud Alert and Security Freeze on your credit files, and obtain[] a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.”<sup>6</sup>

34. On information and belief, Defendant is offering credit monitoring services to individuals who had their Social Security number involved in the Data Breach, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Private Information that cannot be changed, such as Social Security numbers.

35. Even with credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff’s and Class Members’ Private Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

36. Cybercriminals need not harvest a person’s Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff’s and Class Members’ Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create “Fullz” packages, which can then be used to commit fraudulent account activity on Plaintiff’s and the Class’s financial accounts.

37. On information and belief, Defendant failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers’ Private Information. Defendant’s

---

<sup>6</sup> See Sample Notice Letter, available at <https://apps.web.maine.gov/online/aeviewer/ME/40/a6b8d97b-71cf-417b-9585-bdbc8251b836.shtml> (last visited 6/21/2024).

negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Private Information.

***The Value of Private Information***

38. It is well known that Private Information, including Social Security numbers, is an invaluable commodity for which a “cyber black market” exists in which cybercriminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

39. “[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web.”<sup>7</sup>

40. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200<sup>8</sup>; Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web<sup>9</sup>; and other sources report that cybercriminals can also purchase access to entire company data breaches from \$999 to \$4,995.<sup>10</sup>

41. Moreover, Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

---

<sup>7</sup> Consumer Information, Dark Web Monitoring: What You Should Know, Consumer Federation of America (March, 19, 2019), [https://consumerfed.org/consumer\\_info/dark-web-monitoring-what-you-should-know/](https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/).

<sup>8</sup> Anita George, Your personal data is for sale on the dark web. Here’s how much it costs, Digital Trends (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

<sup>9</sup> Brian Stack, Here’s How Much Your Personal Information Is Selling for on the Dark Web, Experian (Dec. 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

<sup>10</sup> VPNOverview, In the Dark, (2019), <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

42. According to the Social Security Administration, each time an individual’s Social Security number is compromised, “the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases.”<sup>11</sup> Moreover, “[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains.”<sup>12</sup>

43. In fact, “[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health.”<sup>13</sup> “Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits.”<sup>14</sup>

44. What’s more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

45. For these reasons, some courts have referred to Social Security numbers as the “gold standard” for identity theft.<sup>15</sup>

---

<sup>11</sup> Avoid Identity Theft: Protect Social Security Numbers, Social Security Admin. – Philadelphia Region, <https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases>

<sup>12</sup> *Id.*

<sup>13</sup> How to Protect Yourself from Social Security Number Identity Theft, Equifax (2014), <https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/>.

<sup>14</sup> Julia Kagan, What Is an SSN? Facts to Know About Social Security Numbers, Investopedia (Feb. 15, 2024) <https://www.investopedia.com/terms/s/ssn.asp>.

<sup>15</sup> *See, e.g., Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111, 2019 WL 7946103, at \*12 (D. Mass. Dec. 31, 2019) (“Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . Access to Social Security numbers causes long-lasting jeopardy because the

46. Similarly, driver’s license numbers, which were also compromised in the Data Breach, are incredibly valuable. “Hackers harvest license numbers because they’re a very valuable piece of information.”<sup>16</sup>

47. A driver’s license can be a critical part of a fraudulent, synthetic identity—which can go for about \$1200 on the dark web. On its own, a forged license can sell for around \$200.<sup>17</sup>

48. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”<sup>18</sup>

49. A study by Experian found that the average cost of medical identity theft is “about \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.<sup>19</sup> Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-

---

Social Security Administration does not normally replace Social Security numbers.”), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also* *McFarlane v. Altice USA, Inc.*, 524 F. Supp. 3d 264, 272 (S.D.N.Y. 2021) (citations omitted) (noting plaintiffs’ Social Security numbers are: arguably “the most dangerous type of personal information in the hands of identity thieves” because it is immutable and can be used to “impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment.” . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, “[a] social security number derives its value in that it is immutable,” and when it is stolen it can “forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.”)

<sup>16</sup> Lee Matthews, Hackers Stole Customers’ License Numbers From Geico In Months-Long Breach, *Forbes* (Apr. 20, 2021), <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658>

<sup>17</sup> *Id.*

<sup>18</sup> Medical I.D. Theft, EFraudPrevention, <https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.>

<sup>19</sup> Elinor Mills, Study: Medical Identity Theft is Costly for Victims, *CNET* (Mar, 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>

third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.<sup>20</sup>

50. 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. There, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” as it is difficult and/or undesirable to change one’s Social Security number, PHI, date of birth, or name.

***Cyberattacks Put Consumers at an Increased Risk of Fraud and Identity Theft.***

51. The link between a data breach and the risk of identity theft is simple and well established. Cybercriminals acquire and steal Private Information to monetize the information. Cybercriminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

52. Cybercriminals can post stolen Private Information on the dark web for years following a data breach, thereby making such information publicly available.

53. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.<sup>21</sup> This gives thieves ample time to commit acts of fraud under the victim’s name.

54. Identity theft victims must therefore spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.

---

<sup>20</sup> Brian O’Connor, Healthcare Data Breach: What to Know About them and What to Do After One, Experian (March 31, 2023) <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>.

<sup>21</sup> Medical ID Theft Checklist, IdentityForce (Jan. 11, 2023) <https://www.identityforce.com/blog/medical-id-theft-checklist-2>.

55. It is within this context that Plaintiff must now live with the knowledge that her Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

***The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.***

56. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting consulting firms that collect and store Private Information, like Defendant, preceding the date of the breach.

57. Data breaches, including those perpetrated against consulting firms that store Private Information in their systems, have become widespread.

58. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.<sup>22</sup>

59. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), and numerous others,<sup>23</sup> Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

---

<sup>22</sup> Q3 2023 Data Compromise Charts, ID Theft Resource Center (2023) <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>.

<sup>23</sup> Michael Hill and Dan Swinhoe, The 15 Biggest Data Breaches of the 21st Century, CSO Online (Nov. 8, 2022), <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.

60. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”<sup>24</sup>

61. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep consumer’s data secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

62. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

63. In October 2019, the FBI published online an article titled “High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations” that, among other things, warned that “[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.”<sup>25</sup>

64. In April 2020, in an article titled “Ransomware mentioned in 1,000+ SEC filings

---

<sup>24</sup> 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>.

<sup>25</sup> High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations, FBI (Oct. 2, 2019) <https://www.ic3.gov/media/y2019/psa191002>.

over the past year,” ZDNet reported that “[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay.”<sup>26</sup>

65. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a “Ransomware Guide” advising that “[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.”<sup>27</sup>

66. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

67. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted Private Information of thousands of its current and former consumers in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Private Information and Defendant’s type of business had cause to be particularly on guard against such an attack.

68. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff’s and Class Members’ Private Information could be accessed,

---

<sup>26</sup> Catalin Cimpanu, Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet (April 30, 2020) <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/>.

<sup>27</sup> Ransomware Guide, U.S. CISA, <https://www.cisa.gov/stopransomware/ransomware-guide>.

exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

69. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its consumers' Social Security numbers and other sensitive data elements within the Private Information to protect against their publication and misuse in the event of a cyberattack.

***Plaintiff's Experience and Injuries***

70. Plaintiff is a current patient of Defendant who underwent eye surgery performed by the Defendant and has paid the Defendant a co-pay and provided her PII to Defendant as a condition of obtaining medical services. Upon information and belief, Plaintiff's Private Information was and continues to be stored and maintained by Defendant.

71. Plaintiff values her privacy and makes every effort to keep her personal information private. She diligently maintains her PII. She has never had her PHI stolen in the past.

72. Plaintiff only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant was obligated to and would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

73. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff was impacted and suffered injury.

74. Plaintiff has been injured in a number of ways, including by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

75. As a result of the Data breach, Plaintiff has stepped up her efforts to protect her Private Information, including by updating and checking credit monitoring service CreditWise, changing passwords, adding alerts and multi-factor authentication to her accounts, and changing payment cards. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

76. Furthermore, Plaintiff has been a victim of fraud transactions on her payment cards since June of 2023, including both her bank and credit cards, which required her to take steps to add pin-codes and otherwise secure her accounts and change cards. Upon information and belief, these fraudulent transactions occurred because of the Data Breach.

77. In addition, she has experienced an increase in spam emails, calls and text messages as a result of the Data Breach, many of which are actively seeking to steal money and information from her.

78. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

79. As a result of the actual harm she has suffered and the present and increased imminent risk of future harm, Plaintiff spent time monitoring her accounts, changing her cards, and reviewing her account statements weekly.

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

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

82. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

***Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft.***

83. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendant.

84. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their Private Information is used;
- b. The diminution in value of their Private Information;
- c. The compromise and continuing publication of their Private Information;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended 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 identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen Private Information; and
- h. The continued risk to their Private Information, which remains in the possession

of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in its possession.

85. The value of Plaintiff's and Class Member's Private Information on the black market is considerable. One such example of cybercriminals using consumer's stolen data for profit is the development of "Fullz" packages.<sup>28</sup>

86. "Fullz" packages are the result of cybercriminals cross-referencing two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

87. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Member's numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cybercriminals in the Data Breach, cybercriminals can easily create a "Fullz" package and sell it at a higher price to unscrupulous operators and criminals (such

---

<sup>28</sup> "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-/>(<https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/>).

as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and Class Members stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

88. Defendant disclosed the Private Information of Plaintiff and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiff and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

89. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated their injuries by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

***Defendant Failed to Adhere to FTC Guidelines.***

90. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("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 the FTCA.

91. 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.

92. 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.<sup>29</sup> The guidelines explain that businesses should:

- 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;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

93. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

94. The FTC recommends that companies not maintain information 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 for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

95. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

96. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information constitutes an unfair act or practice

---

<sup>29</sup> Protecting Personal Information – A Guide for Business, United States Federal Trade Comm'n (2016) <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>.

prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

***Defendant Failed to Follow Industry Standards.***

97. Data breaches are preventable.<sup>30</sup> As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, “In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.”<sup>31</sup> She added that “[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . .”<sup>32</sup>

98. “Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.”<sup>33</sup>

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

100. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email

---

<sup>30</sup> Lucy L. Thomson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at <https://lawcat.berkeley.edu/record/394088>.

<sup>31</sup>*Id.* at 17.

<sup>32</sup>*Id.* at 28.

<sup>33</sup>*Id.*

management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

101. Defendant failed to meet the minimum standards of any 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.

***Defendant Fails to Comply With HIPAA Guidelines.***

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

103. Defendant is a business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

104. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).<sup>34</sup> See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

105. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health*

---

<sup>34</sup> HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

*Information* establishes national standards for the protection of health information.

106. HIPAA’s Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

107. HIPAA requires “compl[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

108. “Electronic protected health information” is “individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R. § 160.103.

109. HIPAA’s Security Rule requires Defendant to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

110. HIPAA also requires Defendant to “review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to “[i]mplement 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.” 45 C.F.R. § 164.312(a)(1).

111. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

112. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*”<sup>35</sup>

113. HIPAA requires a business associate to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the business associate or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

114. HIPAA requires a business associate to mitigate, to the extent practicable, any harmful effect that is known to the business associate of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

115. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost

---

<sup>35</sup> Breach Notification Rule, U.S. Dep’t of Health & Human Services (July 26, 2013) <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.”<sup>36</sup> The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.”<sup>37</sup>

### CLASS ACTION ALLEGATIONS

116. Plaintiff is suing on behalf of herself and the proposed Classes (together the “Class”), defined as follows:

**Nationwide Class: All individuals residing in the United States whose Private Information was compromised in Defendant’s Data Breach, including all those who received a Notice Letter.**

**Colorado Subclass: All individuals residing in Colorado whose Private Information was compromised in Defendant’s Data Breach, including all those who received a Notice Letter.**

117. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

118. Plaintiff reserves the right to amend the Class definitions.

119. This action satisfies the numerosity, commonality, adequacy, and appropriateness requirements under Fed. R. Civ. P. 23:

a. **Numerosity**. Plaintiff’s claims are representative of the proposed Class, consisting of at nearly 378,000 individuals, far too many to join in a single action;

---

<sup>36</sup> Security Rule Guidance Material, U.S. Dep’t of Health & Human Services (Feb. 16, 2024) <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

<sup>37</sup> Guidance on Risk Analysis, U.S. Dep’t of Health & Human Services (July 22, 2019) <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>.

b. **Ascertainability**. Class Members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Plaintiff's interest does not conflict with Class Members' interests, and Plaintiff has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class Members. Indeed, it will be necessary to answer the following questions:

- i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff and the Class's Private Information;
- ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- iii. Whether Defendant was negligent in maintaining, protecting, and securing Private Information;
- iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Private Information;
- v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- vi. Whether Defendant's Notice Letter was reasonable;

- vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;
- viii. What the proper damages measure is; and
- ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

120. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

**FIRST CLAIM FOR RELIEF**  
**Negligence**  
**(On Behalf of Plaintiff and the Class)**

121. Plaintiff re-alleges and incorporates the allegations in paragraphs 1 through 120 as if fully set forth herein.

122. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

123. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure to use adequate data security in accordance with industry standards for data security would compromise the Private Information in its custody in a data breach. And here, that foreseeable danger came to pass.

124. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if their Private Information was wrongfully disclosed.

125. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices.

After all, Defendant actively sought and obtained Plaintiff's and Class Members' Private Information.

126. Defendant owed at least the following duties to Plaintiff and Class Members:

- a. to exercise reasonable care in handling and using the Private Information in its care and custody;
- b. to implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized access;
- c. to promptly detect attempts at unauthorized access; and
- d. to notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their Private Information.

127. Also, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. Such duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

128. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

129. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

130. By being entrusted by Plaintiff and the Class to safeguard their Private Information, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their Private Information with the understanding that Defendant would take appropriate

measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

131. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information—whether by malware or otherwise.

132. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

133. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

134. Defendant breached these duties as evidenced by the Data Breach.

135. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' Private Information by:

- a. disclosing and providing access to this information to third parties; and,
- b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

136. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the Private Information of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injury.

137. Defendant further breached its duties by failing to provide reasonably timely notice

of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Class Members' injuries-in-fact.

138. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

139. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

140. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

**SECOND CLAIM FOR RELIEF**  
**Negligence *per se***  
**(On Behalf of Plaintiff and the Class)**

141. Plaintiff re-alleges and incorporates the allegations in paragraphs 1 through 120 as if fully set forth herein.

142. Under the FTCA, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

143. 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 Defendant, of failing to use reasonable measures to protect the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTCA also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive Private Information.

144. Defendant breached its respective duties to Plaintiff and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

145. Defendant violated its duty under Section 5 of the FTCA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

146. The harm that has occurred is the type of harm the FTCA is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

147. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class Members would not have been injured.

148. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

149. Defendant's violations and its failure to comply with applicable laws and

regulations constitutes negligence *per se*.

150. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed, *supra*).

**THIRD CLAIM FOR RELIEF**  
**Breach of Third-Party Beneficiary Contract**  
**(On Behalf of Plaintiff and the Class)**

151. Plaintiff re-alleges and incorporates the allegations in paragraphs 1 through 120 as if fully set forth herein.

152. Defendant entered into various contracts with its clients, to provide services to its clients.

153. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

154. Defendant knew that if it were to breach these contracts with its clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their Private Information.

155. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' Private Information.

156. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant's failure to use reasonable data security measures to store their Private Information, including but not limited to, the actual harm through the loss of their Private Information to cybercriminals.

157. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

**FOURTH CLAIM FOR RELIEF**  
**Unjust Enrichment**  
**(On Behalf of the Plaintiff and the Class)**

158. Plaintiff re-alleges and incorporate the allegations in paragraphs 1 through 120 as if fully set forth herein.

159. This claim is pled in the alternative to Plaintiff's Third Claim for Relief (breach of third-party beneficiary contract).

160. Plaintiff and Class Members conferred a benefit upon Defendant in providing their Private Information to Defendant.

161. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members. And Defendant benefited from receiving Plaintiff's and Class Members' Private Information, as this was used to facilitate its business.

162. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

163. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

164. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant had they known Defendant would not adequately protect their

Private Information.

165. Defendant should be compelled to establish a common fund to benefit Plaintiff and members of the Class for all unlawful or inequitable proceeds it received as a result of its conduct and Data Breach alleged here.

**FIFTH CLAIM FOR RELIEF**  
**Invasion of Privacy**  
**(On Behalf of the Plaintiff and the Class)**

166. Plaintiff re-alleges and incorporates the allegations in paragraphs 1 through 120 as if fully set forth herein.

167. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

168. Defendant owed a duty to the consumers whose data it retained, including Plaintiff and the Class, to keep such data confidential.

169. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' Private Information is highly offensive to a reasonable person.

170. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

171. The Data Breach constitutes an intentional interference with Plaintiff and the Class's interests in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

172. Defendant acted with a knowing state of mind when it permitted the Data Breach

because it knew its information security practices were inadequate.

173. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

174. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

175. As a proximate result of Defendant's acts and omissions, the Private Information of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

176. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class because their Private Information is still maintained by Defendant with its inadequate cybersecurity system and policies.

177. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiff and the Class.

178. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of her credit history for identity theft and fraud, plus prejudgment interest and costs.

#### **PRAYER FOR RELIEF**

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;
- E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting such other or further relief as may be appropriate under the circumstances.

**JURY DEMAND**

Plaintiff hereby demands that this matter be tried before a jury.

Dated: June 21, 2024

Respectfully submitted,

/s/ Jeff Ostrow  
Jeff Ostrow  
Ken Grunfeld\*  
Kristen Lake Cardoso\*

**KOPELOWITZ OSTROW P.A.**

One W. Las Olas Blvd., Suite 500

Fort Lauderdale, Florida 33301

(954) 525-4100

[ostrow@kolawyers.com](mailto:ostrow@kolawyers.com)

[grunfeld@kolawyers.com](mailto:grunfeld@kolawyers.com)

[cardoso@kolawyers.com](mailto:cardoso@kolawyers.com)

*Counsel for Plaintiff and the Putative Class*

*\*pro hac vice forthcoming*