

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

ELIZABETH ANNE SANCHEZ,
individually and on behalf of all others
similarly situated,

Plaintiff,

v.

VISIONWORKS OF AMERICA, INC.,

Defendant.

Case No.: 5:24-cv-1465

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Elizabeth Anne Sanchez, individually and on behalf of all others similarly situated, for his Class Action Complaint, bring this action against Visionworks of America, Inc. (“Visionworks”) based on personal knowledge and the investigation of counsel and alleges as follows:

I. INTRODUCTION

1. On or around October 10, 2024, an unknown actor gained access to Defendant’s inadequately protected computer systems. As a result, approximately 39,825 individuals, including Plaintiff and the Class Members (as further defined below), have had their personal identifiable information (“PII”) and private health information (“PHI”) (collectively, “Private Information”)¹ exposed (the “Data Breach”).²

¹ Personal identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

² <https://data.the-leader.com/health-care-data-breaches/visionworks-of-america-inc-tx-39825-20241010-hacking-email/>

2. Visionworks is an American company that manages over 700 optical retail stores throughout the United States.

3. Plaintiff and members of the class are current or former patients and/or current or former employees of Defendant. In order to obtain Defendant's services or employment, Defendant required Plaintiff and the Class Members to provide their PII, including their names, dates of birth, email addresses, addresses, Social Security numbers, financial account information, medical information, and other personal information.

4. In carrying out its business, Defendant obtains, collects, uses, and derives a benefit from the Private Information of Plaintiff and the Class. As such, Defendant assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or around October 10, 2024, an unauthorized third party obtained access and exfiltrated data from its servers containing Private Information.

6. It wasn't until months later, on or around December 2024, that Defendant began notifying the public of the Data Breach. Defendant has yet to notify the individuals affected by the Data Breach.

7. Due to the Defendant's negligence, cybercriminals obtained everything they needed to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

8. This class action seeks to redress Defendant's unlawful, willful and wanton failure to protect the personal identifiable information of likely thousands of individuals that was exposed in a major data breach of Defendant's network in violation of its legal obligations.

9. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Plaintiff and Class Members will have to spend time responding to the breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the data breach. Plaintiff and Class Members have incurred and/or will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damage credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

10. Defendant betrayed the trust of Plaintiff and the other Class Members by failing to properly safeguard and protect their personal identifiable information and thereby enabling cybercriminals to steal such valuable and sensitive information.

11. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and other remedies this Court deems proper.

II. THE PARTIES

12. Plaintiff Sanchez is a citizen of Arizona.

13. Visionworks is an American corporation with its headquarters located in San Antonio, Texas.

14. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

15. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

16. This Court has diversity jurisdiction over this action under 28 U.S.C. § 1332(b) because Plaintiff and Defendant are citizens of separate states and the amount in controversy exceeds \$75,000.00 exclusive of interests and costs.

17. This Court has personal jurisdiction over Defendant because Defendant's headquarters are located in this District and Defendant conducts most of its business in this District.

18. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant headquarters are located in this District and it conducts much of its business through this District, including Defendant collecting and/or storing the PII/PHI of Plaintiff and Class Members.

IV. FACTUAL ALLEGATIONS

A. BACKGROUND

19. Visionworks provide optical care across the United States, including glasses, contact lenses, and other vision services and products.

20. In order to provide services or employment, Defendant requires Plaintiff's and Class Members' Private Information, including their names, dates of birth, email addresses, physical addresses, Social Security numbers, medical information, and financial account information.

21. Defendant collected, stored, and maintained the Private Information of Plaintiff and the Class Members on its network. Defendant, however, failed to take reasonable and necessary steps to ensure that its network was secure.

22. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

23. Defendant recognized these duties and made express promises to Plaintiff and the Class Members that it would keep their Private Information secure.

24. Defendant's Privacy Policy states: "We have implemented physical, electronic, and administrative procedures to help safeguard and prevent unauthorized access, maintain data security, and correctly use the information we collect online."³

25. Plaintiff and the Class Members did not have control over how Defendant stored and maintained their Private Information. Rather, Plaintiff was at Defendant's mercy, as Defendant had sole control and authority over its protection of Plaintiff's and the Class Members' Private Information.

26. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

27. Plaintiff and other Members of the Class entrusted their Private Information to Defendant.

28. Plaintiff and Class Members relied on this sophisticated Defendant to keep their Private Information confidential and securely maintained, to use for information for business purposes only, and to only make authorized disclosures of this information. Plaintiff and Class Members demanded security to safeguard their Private Information.

³ <https://www.visionworks.com/privacy-statement#security>

29. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and the Class Members from involuntary disclosure to third parties.

30. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its consumers' Private Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. Rather, Defendant chose to store Plaintiff's and the Class Members' Private Information on an unsecure network, leaving their Private Information vulnerable for cybercriminals to take. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to Plaintiff's and the Class Members' Private Information.

B. THE DATA BREACH

31. On or around October 10, 2024, due to Defendant's failure to maintain an adequate security system, an unknown hacker gained access to Defendant's systems and acquired certain files and information, including Plaintiff and Class Members' Private Information.

32. Defendant negligently delayed in responding to the data breach and informing Plaintiff and the Class Members of the Data Breach.

33. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of individuals like Plaintiff and Class Members.

34. In its notice to the Health and Human Services department, Defendant admitted that an unauthorized actor accessed sensitive information about Plaintiff and Class Members.

35. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur have not been shared with

regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

36. The unencrypted Private Information of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

37. Defendant was negligent and did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of Private Information for Plaintiff and Class Members.

38. Because Defendant had a duty to protect Plaintiff's and Class Members' Private Information, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

39. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect patients' and customers' PII/PHI;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

- e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;
- f. Failing to ensure the confidentiality and integrity of electronic PII/PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII/PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII/PHI in violation of 45 C.F.R. § 164.306(a)(2);
- k. Failing to protect against reasonably anticipated uses or disclosures of electronic PII/PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);
- m. Failing to train all members of its workforces effectively on the policies and procedures regarding PII/PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation

of 45 C.F.R. § 164.530(b);

- n. Failing to render the electronic PII/PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PII/PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR § 164.304’s definition of “encryption”);
- o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
- p. Failing to adhere to industry standards for cybersecurity as discussed above; and
- q. Otherwise breaching its duties and obligations to protect Plaintiff’s and Class Members’ Private Information.

40. Defendant negligently and unlawfully failed to safeguard Plaintiff’s and Class Members’ Private Information by allowing cyberthieves to access Defendant’s computer network and systems which contained unsecured and unencrypted Private Information.

41. Accordingly, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

C. THE DATA BREACH WAS FORESEEABLE

42. In the months immediately preceding the Data Breach, Defendant knew or should have known that Defendant’s computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

43. In October 2019, the Federal Bureau of Investigation 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.”⁴

44. In April 2020, ZDNet reported, in an article titled “Ransomware mentioned in 1,000+ SEC filings over the past year,” 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.”⁵

45. 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.”⁶

46. Medical facilities, such as Defendant, collect and store large amounts of critical, highly valuable corporate records.

⁴ FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* <https://www.ic3.gov/Media/Y2019/PSA191002> (last visited Jan. 25, 2022).

⁵ ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last visited Jan. 25, 2022).

⁶ U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Jan. 25, 2022).

47. More than 144 million Americans' medical information was stolen or exposed in 2023 in a record-breaking number of health care data breaches.

48. Health care organizations are required by law to report to Health and Human Services any security breaches that expose patient information.

49. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that: (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

50. Considering the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted Private Information of Plaintiff and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII/PHI, and Defendant's type of business had cause to be particularly on guard against such an attack.

51. Prior to 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, exfiltrated, and published as the result of a cyberattack.

52. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the 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.

D. THE DATA BREACH WAS PREVENTABLE

53. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

54. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁷

55. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- d. Configure firewalls to block access to known malicious IP addresses.
- e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- f. Set anti-virus and anti-malware programs to conduct regular scans automatically.
- g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

⁷ See *How to Protect Your Networks from RANSOMWARE*, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited July 17, 2023).

- h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
 - i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
 - j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the “AppData/LocalAppData” folder.
 - k. Consider disabling Remote Desktop protocol (RDP) if it is not being used.
 - l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
 - m. Execute operating system environments or specific programs in a virtualized environment.
 - n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁸
56. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- (1) **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .
- (2) **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .

⁸ *Id.* at 3-4.

- (3) **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- (4) **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it. . . .
- (5) **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- (6) **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- (7) **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .⁹

57. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Security internet-facing assets

- Apply latest security updates.
- Use threat and vulnerability management.
- Perform regular audit; Remove privilege credentials.

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise.

Include IT Professionals in security discussions

- Ensure collaboration and among [security operations], [security administrators], and [information technology] administrators to configure servers and other endpoints securely.

Build credential hygiene

⁹ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited July 17, 2023).

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords.
- Apply principle of least-privilege.

Monitor for adversarial activities

- Hunt for brute force attempts.
- Monitor for cleanup of Event logs.
- Analyze logon events.

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection.
- Enable cloud-delivered protection.
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁰

58. Defendant has specifically reported that this Data Breach occurred as a result of an email attack. Email phishing attacks are not new. Defendant could have prevented this Data Breach by training its employees to detect phishing emails. It further could have prevented the Data Breach by creating firewalls should a hacker be able to access the system. Finally, Defendant could have prevented the breach by encrypting Plaintiff's and the Class Members Private Information.

59. Given that Defendant was storing the Private Information of other individuals, Defendant could and should have implemented all the above measures to prevent and detect ransomware attacks.

60. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiff and Class Members.

61. Defendants could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the Private Information of Plaintiff and

¹⁰ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited July 17, 2023).

Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

62. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

63. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

64. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiff's and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized criminal third party.

65. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been

compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents

66. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

E. VALUE OF PRIVATE INFORMATION

67. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. 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 \$200.¹¹ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹² Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹³

68. 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, there, victims can cancel or close credit and debit card accounts. The information

¹¹ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed July 17, 2023).

¹² *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed July 17, 2023).

¹³ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed July 17, 2023).

compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

69. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”¹⁴

70. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

71. One such example of criminals using Private Information for profit is the development of “Fullz” packages.

72. Cyber-criminals can cross-reference 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.

73. 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 the Class’s phone 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 PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a *Fullz* package

¹⁴ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed July 17, 2023).

and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

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

75. Medical information is especially valuable to identity thieves.

76. Theft of PHI, in particular, is 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.”¹⁵

77. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

78. Healthcare data record may be valued at up to \$250 per record on the black market, compared to \$5.40 for the next highest value record (a payment card).¹⁶

79. Because of the value of its collected and stored data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

¹⁵ See Federal Trade Commission, *Medical Identity Theft*, <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited March 18, 2024).

¹⁶ Imprivata, *Hackers, breaches, and the value of healthcare data*, (Jun. 30, 2021), [https://www.imprivata.com/blog/healthcare-data-new-prize-hackers#:~:text=Often%20these%20attacks%20see%20hundreds,record%20\(a%20payment%20card\)](https://www.imprivata.com/blog/healthcare-data-new-prize-hackers#:~:text=Often%20these%20attacks%20see%20hundreds,record%20(a%20payment%20card)) (last visited March 18, 2024).

80. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

F. DEFENDANT IS A HIPAA COVERED ENTITY

81. Defendant is a HIPAA covered entity that provides healthcare and medical services. As a regular and necessary part of its business, Defendant collects and custodies the highly sensitive PII/PHI of its patients and clients' patients. Defendant is required under federal and state law to maintain the strictest confidentiality of the patient's PII/PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

82. As a Defendant covered entity, Defendant is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of PII/PHI, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of PII/PHI, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

83. Due to the nature of Defendant's business, which includes providing a range of medical services, Defendant would be unable to engage in its regular business activities without collecting and aggregating PII/PHI that it knows and understands to be sensitive and confidential.

84. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII/PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII/PHI from unauthorized disclosure.

85. Plaintiff and Class Members are current or former patients and/or customers of Defendant whose PII/PHI was maintained by Defendant, or who received health-related or other services from Defendant, and directly or indirectly entrusted Defendant with their PII/PHI.

86. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII/PHI confidential and securely maintained, to use such PII/PHI solely for business and health care purposes, and to prevent the unauthorized disclosures of the PII/PHI. Plaintiff and Class Members reasonably expected that Defendant would safeguard and keep their PII/PHI confidential.

87. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiff's and Class Members' PII/PHI prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant maintained. Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant data breach.

88. As a HIPAA covered entity that collects, creates, and maintains significant volumes of PII/PHI, the targeted attack was a foreseeable risk of which Defendant was aware and knew it had a duty to guard against. It is well-known that healthcare providers such as Defendant, which collect and store the confidential and sensitive PII/PHI of thousands of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

G. DEFENDANT'S CONDUCT VIOLATES HIPAA OBLIGATIONS TO SAFEGUARD PRIVATE INFORMATION

89. Defendant is a covered entity 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.

90. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

91. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).⁵ See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

92. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

93. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

94. 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.*”¹⁷

95. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services (“HHS”) create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple

¹⁷ <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (last visited March 18, 2024).

regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

96. A Data Breach, such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule. A breach under the HIPAA Rules is defined as:

“...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” *See* 45 C.F.R. 164.40.

97. The Data Breach resulted from a combination of insufficiencies that demonstrate Smile Design failed to comply with safeguards mandated by HIPAA regulations.

H. DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

98. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

99. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to; 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 best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems;

protection against any possible communication system; 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.

102. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

I. DEFENDANT FAILED TO ADHERE TO FTC GUIDELINES

103. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Private Information.

104. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁸ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number,

¹⁸ 17 C.F.R. § 248.201 (2013).

alien registration number, government passport number, employer or taxpayer identification number.”¹⁹

105. 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. The guidelines explain that businesses should:

- a. Protect the sensitive consumer information that they keep;
- b. Properly dispose of PII 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.

106. 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.

107. 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.

108. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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 Federal Trade Commission Act (“FTC Act”),

¹⁹ *Id.*

15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

109. Defendant's negligence and failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff and the Class's Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

J. PLAINTIFF'S EXPERIENCE

110. Plaintiff is a former employee of Defendant. She also purchases a few products from Defendant.

111. In order to receive employment/services, Plaintiff provided Defendant her Private Information, including her name, date of birth, Social Security number, email address, physical address, phone number, medical information, and financial account information. Defendant accepted and stored this Private Information in the regular course of business.

112. After the Data Breach, Plaintiff's Chase Visa card was hacked, resulting in multiple fraudulent charges on her card. Plaintiff also suffered fraudulent charges on her Wells Fargo Checking Account.

113. Armed with Plaintiff's Private Information from the Data Breach, cybercriminals were able to pose as Plaintiff and access her financial account information and steal her hard earned money.

114. As a result of the Data Breach, Plaintiff's sensitive information has been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff will have to worry about when and how his sensitive information may be shared or used to his detriment.

115. As a result of the Data Breach, Plaintiff spent over 15 hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts, reviewing credit reports, and mitigating fraud and identity theft. This time has been lost forever and cannot be recaptured.

116. Additionally, Plaintiff is very careful about not sharing her sensitive Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

117. Plaintiff stores any documents containing her sensitive Private Information in safe and secure locations or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for his various online accounts.

118. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of her privacy.

119. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals.

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

K. PLAINTIFF' AND THE CLASS MEMBERS' INJURIES

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

122. Defendant negligently disclosed the Private Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiff and the Class 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.

123. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's database, amounting to potentially thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

124. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

125. The injuries to Plaintiff and Class Members are directly and proximately caused by Defendant's negligence and failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

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

- a. Identity theft;

- b. Misuse of their PII;
- c. The loss of the opportunity to control how their PII is used;
- d. The diminution in value of their PII;
- e. The compromise and continuing publication of their PII;
- f. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- g. Loss 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 spend researching how to prevent, detect, contest, and recover form identity theft and fraud;
- h. Delay in receipt of tax refund monies;
- i. Unauthorized use of stolen PII; and
- j. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

Plaintiff's and the Class Members' PII is Available on the Dark Web

127. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' Private Information with the intent of engaging in misuse of the Private Information, including marketing and selling Plaintiff's and Class Members' Private Information.

128. Plaintiff has already experienced misuse of her Private Information. She did not experience this misuse prior to the Data Breach. Plaintiff reasonably believes that her information has been sold on the Dark Web.

129. Upon information and believe, the unencrypted Private Information of Plaintiff and Class Members is for sale on the dark web because that is the *modus operandi* of hackers.

130. Plaintiff experienced unknown persons misusing her Private Information, attempting to call her to gain more information – a sure sign that her information has been sold on the Dark Web.

131. The dark web is an unindexed layer of the internet that requires special software or authentication to access.²⁰ Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or “surface” web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA’s web address is cia.gov, but on the dark web the CIA’s web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.²¹ This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

132. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, PII like the Private Information at issue here.²² The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of

²⁰ *What Is the dark web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

²¹ *Id.*

²² *What is the dark web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

birth, and medical information.²³ As Microsoft warns “[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others.”²⁴

Plaintiff and the Class Members Have Experienced Misuse

133. As a result of the Data Breach, the unencrypted and detailed Private Information of Plaintiff and the Class Members has fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members, as seen by the increase in spam calls and emails. Unauthorized actors can easily access and misuse Plaintiff’s and Class Members’ Private Information due to the Data Breach. Plaintiff has already experienced misuse of her Private Information as a result of the Data Breach.

134. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals 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 herein.

135. Because a person’s identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

136. For example, armed with just a name and Social Security number, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information

²³ *Id.*; *What Is the dark web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

²⁴ *What is the dark web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

about a victim's identity, such as a person's login credentials or financial account information. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

137. Moreover, the existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

138. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

139. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

140. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

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.^[25]

²⁵ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

141. 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.

142. Even then, new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²⁶

143. Identity thieves can also use Social Security numbers to obtain a driver’s license or official identification card in the victim’s name but with the thief’s picture; use the victim’s name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim’s information. In addition, identity thieves may obtain a job using the victim’s Social Security number, rent a house or receive medical services in the victim’s name, and may even give the victim’s personal information to police during an arrest resulting in an arrest warrant issued in the victim’s name. And the Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for credit lines.²⁷

144. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

A direct financial loss is the monetary amount the offender obtained from misusing the victim’s account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were

²⁶ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Aug. 23, 2024).

²⁷ *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.^[28]

145. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.²⁹

146. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.”³⁰ Yet, Defendants failed to rapidly report to Plaintiff and Class Members that their Private Information was stolen.

Plaintiff’s and the Class Members’ Lost Time

147. Plaintiff and the Class Members have also spent considerable time and will continue to spend considerable time to protect themselves and keep their identities and personal property protected.

148. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.³¹

²⁸ Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP’T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last accessed Jan. 23, 2024).

²⁹ See <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>.

³⁰ *Id.*

³¹ *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS <https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=%20In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour> (last accessed March 18, 2024); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, <https://www.bls.gov/news.release/pdf/wkyeng.pdf> (last accessed May 9 2024) (finding that on average, private-sector workers make \$1,145 per 40-hour work week.).

149. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week; leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"³² Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

150. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

Plaintiff's and the Class Members Heightened Risk of Identity Theft and Ongoing Injuries

151. Cyberattacks and data breaches at healthcare companies and partner companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

152. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."³³

153. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable

³² Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC <https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html> (Nov. 6, 2019) (last accessed May 9, 2024).

³³ See U.S. Gov't Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007), available at <https://www.gao.gov/new.items/d07737.pdf> (last visited March 18, 2024).

information is to monetize it by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

154. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁴

155. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

156. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name

³⁴ See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps> (last visited March 18, 2024).

and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

157. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.³⁵

158. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

159. Additional fraudulent activity resulting from the Data Breach may not come to light for years.

160. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.³⁶

³⁵ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

³⁶ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed July 17, 2023).

161. As a result of the Data Breach, Cybercriminals also have sufficient information to pose as legitimate persons and gain more information from Plaintiff and the Class Members, putting Plaintiff and the Class Members at a continuing risk of identity theft.

162. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

163. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

164. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

165. Defendant's negligence and failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury 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.

166. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

167. To date, Defendant has offered Plaintiff and some Class Members an inadequate amount of credit monitoring services. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here.

168. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims’ names to make purchases or to launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

169. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

170. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.³⁷ The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

³⁷ See Jesse Damiani, *Your Social Security Number Costs \$4 On The dark web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

171. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, if not forever.

172. The retail cost of credit monitoring and identity theft monitoring can cost \$200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII/PHI.

V. CLASS ACTION ALLEGATIONS

173. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Federal Rule of Civil Procedure 23.

174. The Class that Plaintiff seeks to represent is defined as follows:

All individuals whose Private Information may have been accessed and/or acquired in the cyberattack on or around October 10, 2024 (the "Class").

175. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

176. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

177. **Numerosity**: The Class is so numerous that joinder of all members is impracticable. Defendant reported 39,825 individuals were involved in the Data Breach.

178. **Commonality**: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- e. When Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;
- h. 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;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practice by failing to

safeguard the Private Information of Plaintiff and Class Members;

- k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

179. **Typicality:** Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

180. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to, and affect, Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

181. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

182. **Superiority and Manageability:** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

183. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

184. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

185. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

186. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

187. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate.

188. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

- d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- e. 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;
- f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members; and
- g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE (On Behalf of Plaintiff and the Class)

189. Plaintiff incorporates by reference the forgoing paragraphs as though fully set forth herein.

190. Defendant solicited, gathered, and stored Plaintiff's and the Class's Private Information as part of the operation of its business.

191. Upon accepting and storing the PII of Plaintiff and Class Members, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

192. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiff and Class members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

193. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

194. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive Private Information.

195. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data.

196. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

197. Defendant had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff and the Class include:

- a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members'

Private Information was adequately secured from impermissible access, viewing, release, disclosure, and publication;

- b. To protect Plaintiff's and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems;
- c. To implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers; and
- d. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

198. Defendant was the only one who could ensure that its systems and protocols were sufficient to protect the Private Information that Plaintiff and the Class had entrusted to it.

199. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' Private Information. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Private Information in its possession;
- b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;
- c. Failing to adequately train its employees to not store Private Information longer than absolutely necessary;
- d. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's Private Information; and

- e. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions.

200. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

201. As a proximate and foreseeable result of Defendant's negligent and/or grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages.

202. Though Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendant's possession and control.

203. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

204. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

205. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

206. Additionally, Section 5 of the FTC Act 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 Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

207. Defendant violated Section 5 of the FTC Act 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 it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

208. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

209. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

210. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members

211. Defendant's duty to act reasonably in collecting, storing, and maintaining the Private Information, and to use reasonable care in protecting such information arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information that it either affirmatively acquires, maintains, or stores. Industry standards require Defendant to exercise reasonable care with respect to Plaintiff and Class Members by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and Class Members. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, Defendant was the only entity that could adequately protect the data that that it solicited, collected, and stored.

212. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and Class Members; and (viii) present and continuing costs in terms of time, effort, and money that

has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

213. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

214. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

215. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

216. Plaintiff incorporates by reference the forgoing paragraphs as though fully set forth herein.

217. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

218. Defendant expressly agreed to safeguard and protect Plaintiff's and the Class Members Private Information in its Privacy Policy.

219. Plaintiff and Class Members were required to deliver, and did deliver, their Private Information to Defendant as part of the process of obtaining services and employment provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

220. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

221. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

222. When Plaintiff and Class Members paid money and provided their Private Information to their healthcare providers, either directly or indirectly, in the exchange for goods and services, they entered into implied contracts with their healthcare providers and their business partners, including Defendant, and intended and understood that Private Information would be adequately safeguarded as part of that service.

223. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

224. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

225. In delivering their Private Information to Defendant and paying for healthcare services, Plaintiff and Class Members intended and understood that Defendant would adequately

safeguard the data as part of that service.

226. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

227. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

228. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

229. Had Defendant disclosed to Plaintiff and Class Members that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Sensitive Information to Defendant.

230. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

231. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

232. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

233. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial, or alternatively, nominal damages.

COUNT III – UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

234. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

235. This claim is pled in the alternative to Count II Breach of Implied Contract.

236. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their employment and Private Information to derive profit and facilitate its business.

237. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members.

238. Plaintiff and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

239. 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.

240. 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.

241. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class Members' employment and Private Information because Defendant failed to adequately protect their Private Information.

242. Plaintiff and Class Members have no adequate remedy at law.

243. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

COUNT IV – DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

244. Plaintiff incorporates by reference the forgoing paragraphs as though fully set forth herein.

245. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

246. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and the Class's PII/PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their PII/PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII/PHI and remains at imminent risk that further compromises of their PII/PHI

will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

247. Plaintiff and the Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiff's and the Class's Private Information, including Social Security numbers, while storing it in an Internet-accessible environment, and (ii) Defendant's failure to delete Private Information it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Plaintiff and the Class.

248. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure the Private Information of Plaintiff and the Class;
- b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information; and
- c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiff and the Class harm.

249. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' Private Information. Specifically, this injunction should, among other things, direct Defendant to:

- d. Engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

- e. Audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;
- f. Regularly test its systems for security vulnerabilities, consistent with industry standards; and
- g. Implement an education and training program for appropriate employees regarding cybersecurity.

250. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

251. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

252. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

1. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are a proper representative of the Class requested herein;
2. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;
3. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:
 - i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
 - ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
 - iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
 - iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

- v. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services;
 - vi. Ordering that Defendant conduct regular database scanning and securing checks; and
 - vii. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.
4. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;
 5. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and
 6. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues to triable.

Dated: December 23, 2024

Respectfully submitted,

/s/ William B. Federman

William B. Federman

Jessica A. Wilkes

Federman & Sherwood

212 W. Spring Valley Road

Richardson, Texas 75081

Telephone: (405) 235-1560

E: wbf@federmanlaw.com

E: jaw@federmanlaw.com

*Attorney for the Plaintiff and Proposed
Lead for the Class*

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

ELIZABETH ANNE SANCHEZ, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Maricopa County (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

William B. Federman, Federman & Sherwood 212 W. Spring Valley Rd, Richardson TX 75081

DEFENDANTS

VISIONWORKS OF AMERICA, INC.,

County of Residence of First Listed Defendant (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff, 2 U.S. Government Defendant, 3 Federal Question (U.S. Government Not a Party), 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, PTF DEF, 1 1, 2 2, 3 3, 4 4, 5 5, 6 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: Nature of Suit Code Descriptions.

Table with columns: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES. Includes various legal codes and descriptions.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding, 2 Removed from State Court, 3 Remanded from Appellate Court, 4 Reinstated or Reopened, 5 Transferred from Another District, 6 Multidistrict Litigation - Transfer, 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): Class Action Fairness Act, 28 U.S.C. § 1332(d)(2)

Brief description of cause: Negligence due to Data Breach

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ 5000000 CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER

DATE 12/23/2024 SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.