Exhibit A

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE

IN RE: NUMOTION DATA INCIDENT LITIGATION,	**Case No. 3:24-cv-545** **Judge Aleta A. Trauger**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Shaun Ducrepin and Dulcie Walker ("Plaintiffs"), on behalf of themselves and all others similarly situated ("Class Members"), allege the following against Defendant United Seating and Mobility, LLC d/b/a Numotion ("Defendant"), upon Plaintiffs' personal knowledge and upon information and belief, including the investigation of counsel.

I. INTRODUCTION

1. This action arises from Defendant's failure to safeguard the personally identifiable information[1] ("PII") and protected health information ("PHI") (PII and PHI together, "Private Information") of Plaintiffs and the proposed Class Members, thousands of Defendant's current and former employees and patients. Specifically, between February 29, 2024, and March 2, 2024, the notorious criminal ransomware group known as Black Basta accessed Defendant's network systems and exfiltrated Plaintiffs' and Class Members' Private Information stored therein, including their names, dates of birth, Social Security numbers, identification documents, employment information, medical equipment order details, supporting medical documentation, and health insurance information, causing widespread injury and damages to Plaintiffs and Class

[1] The Federal Trade Commission defines "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, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

Members (the "Data Breach").

2. According to its website, Defendant "is the nation's largest and leading provider of products and services to help individuals with mobility limitations," furnishing Complex Rehab Technology products and accessories, innovative lifestyle products, service and repair, catheters, wheelchair accessible vehicles, and other services for individuals with mobility challenges.[2]

3. As a condition of receiving medical equipment products and/or employment from Defendant, Plaintiffs and Class Members were required to entrust Defendant with their sensitive Private Information including their names, passports or drivers' licenses, dates of birth, Social Security numbers, medical equipment information, medical treatment and diagnosis information, and health insurance information.

4. As the custodian of Plaintiffs' and Class Members' Private Information it collected and maintained, Defendant had a duty to adopt reasonable measures to protect such Private Information from involuntary disclosure to unauthorized third parties, and to keep it safe and confidential. Defendant had obligations under contract, statutory and common law, industry standards, and representations made to Plaintiffs and Class Members to keep their Private Information secure and to protect it from unauthorized access and disclosure.

5. Defendant breached these duties owed to Plaintiffs and Class Members by failing to safeguard their Private Information that it collected and maintained, including by failing to implement industry standards for data security to protect against cyberattacks, resulting in the Data Breach.

6. According to Defendant's April 15, 2024, letter[3] notifying individuals whose

[2] *See* https://www.numotion.com/about-us (last visited July 9, 2024).

[3] *See* Defendant's Data Breach Notification to Maine Attorney General, available at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e5e83591-a395-42ca-b1a7-7b1330b08acc.shtml; Numotion Sample Notice of

Private Information was compromised in the Data Breach ("Notice Letter"), between approximately February 29 and March 2, 2024, an unnamed, unauthorized cybercriminal accessed Defendant's information systems and stole files containing Plaintiffs' and Class Members' Private Information.

7. Although Defendant discovered the Data Breach on or about March 2, 2024, it failed to notify and warn Plaintiffs and Class Members of the unauthorized disclosure of their Private Information until April 15, 2024, over six weeks later.

8. As a direct result of the Data Breach, which Defendant failed to take reasonable steps to prevent, the Private Information of Defendant's customers and employees, including Plaintiffs and Class Members, was stolen by notorious cybercriminals.

9. Plaintiffs have now discovered that the Black Basta ransomware group published the Private Information stolen in the Data Breach on its Dark Web page, where, as of July 9, 2024, it has already been viewed over 10,000 times.

10. Plaintiffs and Class Members now face a lifetime risk of identity theft due to the nature of the Private Information stolen and now disseminated, which they cannot change, and which cannot be made private again.

11. Defendant's harmful conduct has injured Plaintiffs and Class Members in multiple ways, including, *inter alia* (i) actual identity theft, and the imminent risk thereof; (ii) the lost or diminished value of their Private Information; (iii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) out-of-pocket expenses and lost opportunity costs to mitigate the Data Breach's consequences, including lost time; (v) loss of privacy, including through the publication and dissemination of their Private

Security Incident, attached as Exhibit A.

Information on the Dark Web; (vi) loss of the benefit of their bargain with Defendant; and (vi) emotional distress associated with the loss of control over their highly sensitive Private Information and attendant, certain risk of identity theft and fraud.

12. Defendant's failure to protect Plaintiffs' and Class Members' Private Information has harmed and will continue to harm thousands of Defendant's current and former patients and employees, causing Plaintiffs to seek relief on a class-wide basis.

13. Plaintiffs bring this action on behalf of themselves and all others similarly situated, the proposed Class of persons whose Private Information was compromised in the Data Breach, asserting causes of action for (I) Negligence; (II) Negligence *Per Se*; (III) Breach of Implied Contract; (IV) Breach of Confidence; (V) Unjust Enrichment; (VI) Invasion of Privacy/Intrusion Upon Seclusion; and (VII) Bailment, seeking an award of monetary damages and injunctive and declaratory relief, due to Defendant's failure to adequately protect Plaintiffs and Class Members' highly sensitive Private Information.

II. PARTIES

12. Plaintiff Shaun Ducrepin is a natural person, resident, and citizen of Minnesota. Plaintiff Ducrepin is a former employee of Defendant, having worked for Defendant from 2021–2024, and was/is a victim of Defendant's Data Breach.

13. Plaintiff Dulcie Walker is a natural person, resident, and citizen of Arkansas. Plaintiff Walker is a customer of Defendant whose information was affected by the Data Breach.

14. Defendant United Seating and Mobility, LLC d/b/a Numotion is a limited liability company formed under the laws of Missouri, with its headquarters at 155 Franklin Road, Suite 300, Brentwood, Tennessee, 37027. Defendant has thousands of customers and employees located throughout the United States.

III. JURISDICTION AND VENUE

15. This Court has personal jurisdiction over Defendant because its principal place of business is in Tennessee and, personally or through its agents, it engages in substantial and continuous activities in Tennessee and conducts business in this state.

16. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because the amount in controversy exceeds $5 million, exclusive of interest and costs, the number of Class Members is over 100, and at least one Class Member is a citizen of a state that is diverse from Defendant's citizenship, namely, Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

17. The Court has supplemental jurisdiction over Plaintiffs' claims arising under state law pursuant to 28 U.S.C. § 1367.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant has its principal place of business located in this District, and a substantial part of the events giving rise to this action and Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Defendant's Business

19. According to Defendant's website,

> Numotion is the nation's largest and leading provider of products and services to help individuals with mobility limitations maximize their health, personal independence, and actively participate in everyday life.[4]

20. Defendant has over 150 locations throughout the country, serves over 300,000 individual customers, and has more than 3,100 employees.[5]

---

[4] https://www.numotion.com/about-us (last accessed May 8, 2024).
[5] *Id.*

21. As a condition of receiving healthcare products and services and/or employment from Defendant, Plaintiffs and Class Members were required to entrust Defendant with their sensitive Private Information including names, identification documents, dates of birth, Social Security numbers, medical equipment information, medical treatment and diagnosis information, and health insurance information, and did in fact turn over such Private Information to Defendant.

22. In exchange for receiving Plaintiffs' and Class Members' Private Information, Defendant promised to safeguard the sensitive, confidential data and to only use it for authorized and legitimate purposes.

23. The data held by Defendant and accessed in the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

24. Defendant made promises to Plaintiffs and Class Members to adequately maintain and protect their Private Information, demonstrating its understanding of the importance of securing Private Information.

25. Moreover, Defendant's past experiences should have impressed upon it the need to secure such information. Indeed, Defendant has previously experienced a theft of its technology equipment, including laptops and computers that had inappropriately been used to store sensitive customer information.[6]

26. Defendant made promises and representations to its customers, including Plaintiff Walker and Class Members, that the Private Information it collected would be kept safe and confidential, the privacy of that information would be maintained, and Defendant would delete any sensitive information after it was no longer required to maintain it.

---

[6] *Statement Regarding Theft and Data Breach at the Tacoma, WA Office*, NUMOTION, https://www.numotion.com/about-us/news/statement-regarding-theft-and-data-breach-at-the-t (last visited July 8, 2024).

27. Indeed, Defendant's "Privacy Principles" published on its website promises as follows:

> **We are open and honest in how we use customer data.**
> We use data to offer and provide our customers products that enhance mobility and independence. Nothing more. Nothing less.
>
> **We collect only the data we need.**
> Our customers trust us with their most sensitive data at incredibly vulnerable moments in life. We are grateful for that trust and we will not abuse it.
>
> **We respect and protect our customers' data.**
> We understand that each of us alone gets to choose whom we share our data with. We take steps to protect customer data from unauthorized access or disclosure.[7]

28. Defendant's Notice of Privacy Practices published on its website further promises and warrants to its customer patients as follows, in part:

> We will share your health information within Numotion to carry out our treatment, payment, and health care operations. The law requires us to maintain the privacy of certain health information called "Protected Health Information" ("PHI"). PHI is the information that you provide us or that we create or receive about your health care. When we use or disclose (share) your PHI, we are required to follow the terms of this Notice or other notices in effect at the time we use or share the PHI. Finally, the law provides you with certain rights described in this Notice. Furthermore, we are required to notify you following a breach of unsecured PHI.
> . . .
>
> The information you provide us will/may be shared with other organizations directly related to providing the equipment you need, like hospitals and clinics.
> . . .
> For any purpose other than the ones described above, we may only use or share your PHI when you grant us your written permission (authorization).

[7] https://www.numotion.com/about-us/privacy-principles (last accessed May 31, 2024).

29. None of the above permitted purposes for Defendant's disclosure of Private Information as set forth in its Notice of Privacy Practices include the disclosure to unknown and unauthorized cybercriminals, as in the Data Breach.

30. Additionally, Defendant acknowledges the importance of properly safeguarding its employees' Private Information, maintaining policies on Employee Data Privacy and Proprietary & Confidential Information ("Employee Privacy Policy")[8] in which Defendant promises its employees, including Plaintiff Ducrepin and Class Members, to keep their Private Information safe, as follows:

Employee Data Privacy

BACKGROUND
Special laws and rules protect the privacy and confidentiality of personal data.

CORPORATE PRINCIPLE
Numotion respects the confidentiality of the personal information of employees. This includes medical and personnel records. Access to personal information is only authorized when there is a legitimate and lawful reason, and access is only granted to appropriate personnel. Requests for confidential employee information from anyone outside our company under any circumstances must be approved in accordance with our policies.

MY ROLE
I respect the personal information of my fellow employees. I will not access or seek access to anyone else's personal data, except when absolutely necessary and then only in compliance with company policies and applicable law. When in doubt, I will contact Numotion's Human Resources department or the Legal and Compliance Department.

Proprietary & Confidential Information

BACKGROUND

[8] See Code of Conduct, available at https://secure.ethicspoint.com/domain/media/en/gui/75178/code.pdf (Relevant excerpts are attached as Exhibit B).

> Numotion holds certain information as confidential and proprietary information, or trade secrets, about our Company, our customers, our prospective customers, our payors, or others. This information is a cornerstone of our business success. Unauthorized sharing of this information could lead to significant losses for the Company and to serious civil and criminal consequences for the employee involved.
>
> **CORPORATE PRINCIPLE**
> Numotion takes great care to protect its trade secrets and confidential information. Employees, officers and directors must maintain the confidentiality of all information entrusted to them, except when disclosure is authorized or legally required. Confidential or proprietary information includes, among other things, any non-public information concerning Numotion, including its businesses, financial performance, results or prospects, and any nonpublic information provided by a third party with the expectation that the information will be kept confidential and used solely for the business purpose for which it was conveyed.
>
> **MY ROLE**
> I will handle all Numotion information carefully and will not disclose it to unauthorized persons. I take great care to protect Numotion's trade secrets and confidential information. I will not disclose any Numotion trade secret or confidential information during or after my employment with Numotion except when legally required to do so.

31. The purposes for Defendant's disclosure of Private Information as set forth in the Employee Privacy Policy do not include disclosure to unknown and unauthorized cybercriminals as in the Data Breach.

32. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its promises to safeguard that information, including in the manners set forth in Defendant's Privacy Principles web page, Notice of Privacy Practices, or Employee Privacy Policy.

33. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information,

Defendant could not perform the services it provides.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to Plaintiffs and Class Members, and knew or should have known that it was responsible for protecting their Private Information from unauthorized disclosure.

35. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

36. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard it.

37. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

Defendant Failed to Adequately Safeguard Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

38. Defendant collected and maintained its current and former patients' and employees' Private Information in its computer information technology systems and networks, including when the Data Breach occurred.

39. The information held by Defendant at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

40. On or about May 1, 2024, Defendant began sending Notice Letters notifying Plaintiffs and Class Members of the Data Breach.[9]

[9] *See* Ex. A.

41. The Notice Letter provided in part as follows:

> **What Happened?** On March 2, 2024, we discovered that we were the victim of a cyber-attack. Upon learning of the incident, we promptly began an investigation and worked to secure our systems. We also engaged a forensic security firm to assist with our investigation and confirm the security of our computer systems. The forensic investigation determined that an unknown, unauthorized third party accessed our computer systems between February 29, 2024, and March 2, 2024, and encrypted some of our computer files. The investigation also determined that the third party may have accessed and acquired certain files from our systems during this period.

42. Defendant's Notice Letter further acknowledges that its current and former patients' and employees' sensitive Private Information was accessed in the Data Breach, including the names, dates of birth, photocopied identification documents, Social Security numbers, medical equipment information, medical treatment and diagnosis information, and health insurance information of Plaintiffs and Class Members.

43. Yet, Defendant's Notice Letter fails to inform Plaintiffs and Class Members of critical facts surrounding the Data Breach, omitting details like the extent of Private Information compromised or that it was accessed by the notorious Russian ransomware organization Black Basta, which has now published it on the Dark Web.

44. Defendant did not use reasonable security procedures and practices appropriate to the sensitive and confidential nature of Plaintiffs' and Class Members' Private Information that it collected and maintained, such as encrypting the information or deleting it when it is no longer needed, which caused the theft of that Private Information in the Data Breach.

45. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiffs' and Class Members' Private Information and training its employees on standard cybersecurity practices.

46. For example, if Defendant had of implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that any PII/PHI-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate at least three days of malicious activity in Defendant's information system without alarm bells going off, including the reconnaissance necessary to identify where Defendant stored PII/PHI, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Defendant's system without being caught.

47. The activities detailed in the preceding paragraph would have been recognized by Defendant if it bothered to implement basic monitoring and detection "systems, which then would have stopped the attack or greatly reduced its impact.

48. Additionally, according to the "*#StopRansomware: Black Basta*" whitepaper published by the Joint Cybersecurity Advisory, "Black Basta affiliates use common initial access techniques—such as phishing and exploiting known vulnerabilities."[10] Phishing is a tactic that uses social engineering to send emails containing malicious attachments to targeted organizations or individuals,[11] and relies on user execution (like opening an email or downloading an attachment) to gain access.[12]

49. Had Defendant trained its employees on reasonable and basic cybersecurity topics, like common phishing techniques or indicators of a potentially malicious event, Black Basta would not have been able to carry out the Data Breach through phishing.

---

[10] *See* Fed. Bureau Investigation, et al., *#StopRansomware: Black Basta*, (May 10, 2024), https://www.ic3.gov/Media/News/2024/240511.pdf.
[11] *See* Phishing, MITRE ATT&CK (March 1, 2024), https://attack.mitre.org/versions/v15/techniques/T1566.
[12] *Id.*

50. As a result of Defendant's failures, Plaintiffs' and Class Members' Private Information was stolen in the Data Breach when criminal hackers accessed and acquired files in Defendant's computer systems storing that sensitive information in unencrypted form.

51. Defendant's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiffs' and Class Members' Private Information, meaning Defendant had no effective means in place to detect and prevent attempted cyberattacks.

52. Moreover, despite discovering the Data Breach on March 2, 2024, Defendant waited until April 15, 2024, to report the Data Breach to the Maine Attorney General and other consumer agencies as required, stating that the Data Breach involved an "external system breach (hacking)" affecting 4,190 persons and occurring between February 29, 2024, and March 2, 2024, and which Defendant discovered on March 4, 2024.[13]

53. Notwithstanding Defendant's representation to the Maine Attorney General that the Data Breach affected only 4,190 persons, Defendant reported the U.S. Department of Health and Human Services on May 1, 2024, that the Data Breach affected 602,265 patients.

Defendant Knew or Should Have Known of the Risk of a Cyber Attack Because Businesses like Defendant in Possession of Private Information are Particularly Suspectable.

54. Defendant's negligence, including its gross negligence, in failing to safeguard Plaintiffs' and Class Members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

55. Private Information of the kind accessed in the Data Breach is of great value to

[13] *See*: Numotion's Data Breach Notification to Maine Attorney General, avail. at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e5e83591-a395-42ca-b1a7-7b1330b08acc.shtml.

hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the Dark web.

56. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as his or her name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information connected or linked to an individual such as his or her birthdate, birthplace, and mother's maiden name.

57. Data thieves regularly target entities in the healthcare industry like Defendant due to the highly sensitive information they maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

58. Cyber-attacks against institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[14]

59. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable healthcare provider and employer, should have known that the Private Information it collected and maintained would be targeted by

[14] Tom Kellermann, *Cyber Bank Heists: Threats to the financial sector*, at 5, CONTRAST SECURITY https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf (last accessed July 8, 2024).

cybercriminals.

60. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[15]

61. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[16]

62. Defendant's data security obligations were particularly important given the substantial increase, preceding the date of the subject Data Breach, in cyberattacks and/or data breaches targeting healthcare entities like Defendant that collect and store PHI.

63. For example, of the 1,862 data breaches recorded in 2021, 330 of them, or 17.7%, were in the healthcare industry.[17]

64. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[18]

65. Entities in custody of PHI, like Defendant, reported the largest number of data

---

[15] *See* Identity Theft Resource Center, *2021 Annual Data Breach Report Sets New Record for Number of Compromises*, ITRC (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[16] IBM, *Cost of a data breach 2022: A million-dollar race to detect and respond*, https://www.ibm.com/reports/data-breach (last accessed July 8, 2024).

[17] Identity Theft Resource Center, *2021 Data Breach Annual Report*, ITRC (Jan. 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[18] *Id.*

breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[19] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[20] Almost fifty percent of the victims lost their healthcare coverage as a result of the incident, while nearly thirty percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy.[21]

66. Thus, the healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[22]

67. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[23] A complete identity theft kit with health insurance credentials may be worth

---

[19] *See* Identity Theft Resource Center, *2022 Annual Data Breach Report*, ITRC (Jan. 2023) https://www.idtheftcenter.org/publication/2022-data-breach-report.
[20] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.
[21] *Id.*
[22] *9 reasons why healthcare is the biggest target for cyberattacks*, SECURESWIVEL, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks (last accessed July 8, 2024).
[23] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows* (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[24]

68. Indeed, cyberattacks by the Black Basta group in particular, such as this Data Breach, are a specifically known and acknowledged risk for businesses in the healthcare industry like Defendant. According to a Threat Profile published by the U.S. Department of Health and Human Services Cybersecurity Coordination Center,

> Having already attacked several health and public health sector organizations in 2022, Black Basta is a credible threat to the sector. . . . In these attacks, Black Basta not only affected the websites of specific health information technology, healthcare industry services, laboratory and pharmaceutical, and health plans organizations across multiple states, but also cumulatively stole several gigabytes of data on personal identifiable information (PII) for members of health organizations, their customers, and employees. Continued and future attacks on and unpatched critical vulnerabilities in the public health and healthcare systems sector could be potentially life threatening, the impact of which would be devasting to critical infrastructure.[25]

69. As a healthcare entity in possession of its patient customers' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiffs and Class Members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach or the foreseeable injuries it caused.

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

---

[24] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world* (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[25] *Threat Profile: Black Basta*, U.S. DEP. HEALTH & HUMAN SERVS. (Mar. 15, 2023), available at https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf (last accessed July 9, 2024).

71. Given the nature of the Data Breach, it was foreseeable that Plaintiffs' and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals, including Black Basta specifically, for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiffs' and Class Members' names.

72. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

73. Plaintiffs and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

74. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

75. Moreover, Defendant's previous data breach put Defendant on notice of the importance of meeting its obligations under statute, regulation, and the common law, and the types of harms associated with such data breaches.[26]

Defendant is Required but Failed to Comply with FTC Rules and Guidance.

[26] *Statement Regarding Theft and Data Breach at the Tacoma, WA Office*, NUMOTION, https://www.numotion.com/about-us/news/statement-regarding-theft-and-data-breach-at-the-t (last visited July 8, 2024).

76. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

77. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses like Defendant. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[27]

78. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[28]

79. The FTC further recommends that companies not maintain Private 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.

80. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential

[27] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016),https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 8, 2024).
[28] *Id.*

consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

81. Such FTC enforcement actions include actions against healthcare entities like Defendant. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

82. Section 5 of the FTC Act, 15 U.S.C. § 45, 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.

83. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[29]

84. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

85. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information or to comply

[29] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

Defendant is Required but Failed to Comply with HIPAA Guidelines.

86. 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; and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C.

87. Defendant is further subject to the Health Information Technology Act ("HITECH")'s rules for safeguarding electronic forms of medical information. *See* 42 U.S.C. §17921; 45 C.F.R. § 160.103.

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

89. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

90. HIPAA's Security Rule required and requires that Defendant do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

91. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. §164.312(a)(1).

92. HIPAA and HITECH also obligate Defendant to implement procedures to prevent, detect, contain, and correct data security violations and disclosures of PHI that are reasonably anticipated but not permitted by privacy rules. *See* 45 C.F.R. § 164.306(a)(1), (a)(3).

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

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

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

effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." U.S. Department of Health & Human Services, Security Rule Guidance Material.[30] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology, which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." U.S. Department of Health & Human Services, Guidance on Risk Analysis.[31]

96. As alleged in this Complaint, Defendant failed to comply with HIPAA and HITECH. It failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach, and failed to ensure the confidentiality and protection of Plaintiffs' and Class Members' Private Information, including photocopies of their most personal identification documents and their PHI.

Defendant Failed to Comply with Industry Standards.

97. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

98. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses,

[30] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed July 8, 2024).
[31] *Id.*

Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[32]

99. The NIST also recommends certain practices to safeguard systems, such as the following:

> a. Control who logs on to your network and uses your computers and other devices.
>
> b. Use security software to protect data.
>
> c. Encrypt sensitive data, at rest and in transit.
>
> d. Conduct regular backups of data.
>
> e. Update security software regularly, automating those updates if possible.
>
> f. Have formal policies for safely disposing of electronic files and old devices.
>
> g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[33]

100. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing]

---

[32] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Feb. 9, 2024).

[33] Federal Trade Commission, *Understanding the NIST Cybersecurity Framework*, FTC.GOV, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last accessed July 8, 2024).

that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[34]

101. Upon information and belief, Defendant failed to implement industry- standard cybersecurity measures, including failing to meet the minimum standards of both 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 established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

Defendant Owed Plaintiffs and Class Members a Common Law Duty to Safeguard their Private Information.

102. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being

[34] Cybersecurity & Infrastructure Security Agency, *Shields Up: Guidance for Organizations*, https://www.cisa.gov/shields-guidance-organizations (last accessed July 8, 2024).

compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiffs and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiffs' and Class Members' Private Information.

103. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

104. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

105. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

106. Defendant owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

107. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

108. Defendant tortiously failed to take the precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiffs' and Class Members' rights.

Plaintiffs and Class Members Suffered Damages.

109. Defendant's failure to implement or maintain adequate data security measures for Plaintiffs' and Class Members' Private Information directly and proximately caused injuries to Plaintiffs and Class Members by the consequential disclosure of their Private Information to a

criminal ransomware group in the Data Breach.

110. Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. Plaintiffs and Class Members must immediately devote time, energy, and money to (a) closely monitor their medical statements, bills, records, and credit and financial accounts; (b) change login and password information on any sensitive account even more frequently than they already do; (c) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (d) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

111. The unencrypted Private Information of Plaintiffs and Class Members compromised in the Data Breach has ***already*** been published on the Dark Web by Black Basta. This Private Information published on the Dark Web includes photocopied images of Data Breach victims' passports, drivers' licenses, Social Security cards, and birth certificates, as well as files containing Plaintiffs' and Class Members' PHI and other sensitive Private Information. Unauthorized individuals with nefarious intentions can now easily access Plaintiff's and Class Members' Private Information—and thousands have already done so.

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

113. Once Private Information is exposed, virtually no way exists to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct which caused the Data Breach.

Further, the value of Plaintiffs' and Class Members' Private Information has been diminished by its exposure in the Data Breach.

114. As a result of Defendant's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of Private Information.

115. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud–a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[35]

116. With respect to healthcare breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[36]

117. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[37]

118. The reality is that cybercriminals seek nefarious outcomes from a data breach" and "stolen health data can be used to carry out a variety of crimes."[38]

119. Health information in particular is likely to be used in detrimental ways, including by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and

[35] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last accessed July 8, 2024).
[36] Heather Landi, *More than 70% of hospital data breaches compromise information that puts patients at risk of identity theft* (Sept. 23, 2019, 5:00 PM), https://www.fiercehealthcare.com/tech/more-than-70-hospital-data-breaches-expose-sensitive-information-putting-patients-at-risk.
[37] *Id.*
[38] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

serious and long-term identity theft.[39]

120. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[40]

121. Plaintiffs and Class Members are also at a continued risk because their Private remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack on multiple occasions and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' Private Information.

Plaintiff Shaun Ducrepin's Experience

122. Plaintiff Ducrepin is a former employee of Defendant, having been employed with Defendant from 2021–2024.

123. As a material condition of employment, Plaintiff Ducrepin was required to provide Defendant with his Private Information, including his full name, date of birth, Social Security number, and other employment information.

124. At the time of the Data Breach, Defendant retained Plaintiff Ducrepin's Private Information in its system.

125. On or about April 15, 2024, Plaintiff Ducrepin received Defendant's Notice Letter informing him that his name, date of birth, Social Security number and "employment information" were compromised and unauthorizedly disclosed in the Data Breach.

[39] *Id.*
[40] https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

126. As a result of the Data Breach, Plaintiff Ducrepin has spent considerable time and effort attempting to remediate the harmful effects of the Data Breach, including seeking legal advice in response to the Data Breach, and to prevent fraudulent misuse or damages, as well as time and effort to monitor his accounts to protect himself from additional identity theft.

127. Plaintiff's lost time is a monetary injury and such time was spent at Defendant's direction in that Defendant told Plaintiff to perform such mitigation tasks in its Notice Letter and online notice.[41]

128. Plaintiff Ducrepin fears that his personal financial security is at substantial risk and because of the uncertainty over the information compromised in the Data Breach. He is experiencing feelings of anxiety, stress, and fear because of the Data Breach, which has manifested into sleep disruption. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim the law provides redress for.

129. Plaintiff Ducrepin was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive Private Information and the harm caused by the Data Breach. This has been compounded by Defendant's delay in notifying Plaintiff Ducrepin of the Data Breach. Plaintiff Ducrepin has had to expend the above time and effort to rectify the impacts of the Data Breach and does not know how many more attempts may arise for his lifetime.

130. As a result of Defendant's inadequate data security practices and the resulting Data Breach, Plaintiff Ducrepin faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like his Social Security number.

---

[41] "As a precautionary measure, individuals should remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing their account statements and monitoring credit reports closely. If individuals detect any suspicious activity on an account, they should promptly notify the financial institution or company with which the account is maintained." *Data Privacy Incident*, https://www.numotion.com/data-privacy-incident (last accessed July 8, 2024).

Plaintiff Dulcie Walker's Experience

131. Plaintiff Walker was a former customer of Defendant. To obtain the medical device products offered by Defendant, she was required to provide Defendant with her Private Information.

132. At the time of the Data Breach, Defendant retained Plaintiff Walker's Private Information in its system.

133. Plaintiff Walker is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

134. Plaintiff Walker learned of the Data Breach after reviewing the Notice Letter from Defendant. According to the Notice Letter, Plaintiff Walker's Private Information was improperly accessed and obtained by unauthorized third parties in the Data Breach. She has since discovered that her Private Information was accessed by the Black Basta ransomware group in the Data Breach and has now been published on the Dark Web.

135. The stolen Private Information comprised Plaintiff Walker's name, date of birth, medical equipment order details, supporting medical documentation, and health insurance information.

136. As a result of the Data Breach, Plaintiff Walker made reasonable efforts to mitigate the impact of the Data Breach, including expending time to check her bills and accounts to make sure they were correct, which time she would not have been required to spend on such tasks but for the Data Breach. Plaintiff Walker has spent significant time dealing with the Data Breach, at Defendant's direction, valuable time she otherwise would have spent on other activities, including

but not limited to work and/or recreation. This time has been lost forever, cannot be recaptured, and is a monetary injury that has already occurred.

137. As a result of the Data Breach, Plaintiff Walker fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

138. Plaintiff Walker additionally anticipates spending considerable time and money on an ongoing basis to address the injuries and harms caused by the Data Breach.

139. As a result of the Data Breach, Plaintiff Walker is presently and imminently at risk and will continue to be at such increased risk of identity theft and fraud for years to come.

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

V. COMMON INJURIES AND DAMAGES

141. As the direct and proximate result of Defendant's ineffective and inadequate data security practices and the resulting Data Breach, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

142. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including but not limited to (a) invasion of privacy; (b) out of pocket costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and

loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) out of pocket costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) loss of the benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendant's possession and subject to further breaches, so long as Defendant fails to undertake adequate measures to protect it.

The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing.

143. 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 below.

144. 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 to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

145. 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 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 are often the starting point for these additional targeted attacks on the victims.

146. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[42] 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.[43] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

147. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here. 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 birth, and medical information. As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[44]

148. 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

[42] Louis DeNicola, *What Is the Dark Web?*, EXPERIAN (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web.
[43] *Id.*
[44] *What is the Dark Web?*, MICROSOFT 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

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.[45]

149. 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.

150. 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."[46]

151. 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

[45] Social Security Administration, *Identity Theft and Your Social Security Number*, SSA.GOV (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[46] 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.

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.[47]

152. 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."[48]

153. One such example of criminals using Private Information for profit is the development of "Fullz" packages. 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 to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

154. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' 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 Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as identity thieves or illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and Class Members' stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

---

[47] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[48] *See* Federal Trade Commission, Medical Identity Theft (May 2021), http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

155. 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.[49]

156. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[50] Defendant did not rapidly report to Plaintiffs and the Class that their Private Information had been stolen.

157. 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.

158. 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.

159. 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, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

160. As a result of the recognized risk of identity theft, when a data breach occurs, and

[49] *See 2019 Internet Crime Report Released* (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[50] *Id.*

an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm–yet the asset of time has been lost.

161. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

162. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, 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 will face "substantial costs and time to repair the damage to their good name and credit record."[51] Indeed, the FTC recommends that identity theft victims take several steps and spend time 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.[52]

Diminution of Value of the Private Information

[51] *See* U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 2 (June 2007), https://www.gao.gov/new.items/d07737.pdf ("GAO Report").
[52] *See* Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed July 8, 2024).

163. Private Information is a valuable property right.[53] Its value is axiomatic, considering the value of Big Data in corporate America and 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.

164. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information 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.

165. Private Information can sell for as much as $363 per record according to the Infosec Institute.[54]

166. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data sells on the dark web for $50 and up.[55]

167. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[56] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[57]

---

[53] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, 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).

[54] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market.

[55] *Ransomware attacks paralyze, and sometimes crush, hospitals*, SOPHOS NEWS (Oct. 3, 2019), https://news.sophos.com/en-us/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals

[56] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak* (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[57] https://datacoup.com/.

Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[58]

168. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized release onto the Dark web, where it is now available for additional criminals to access and holds significant value for the threat actors.

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

169. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered because of the Data Breach.

170. Black Basta has already published Private Information exfiltrated in the Data Breach on the Dark Web. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been or will be further disseminated on the black market/Dark Web for sale and purchase by bad actors 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).

171. 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.

[58] Nielsen Computer & Mobile Panel, Frequently Asked Questions, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

172. 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.[59] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers and birth certificate photocopies).

173. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

174. 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 Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of Benefit of the Bargain

175. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain.

176. When agreeing to provide their Private Information, which was a condition precedent to obtain products and services from Defendant, and paying Defendant, directly or indirectly, for its services, Plaintiff Walker and Class Members, as patients and consumers, understood and expected that they were, in part, paying for services and data security to protect the Private Information they were required to provide.

177. When agreeing to provide their Private Information, which was a condition

[59] *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.

precedent to obtain employment and compensation from Defendant, Plaintiff Ducrepin and Class Members, as current and former employees, understood and expected that they were being compensated, in part, commensurate with Defendant's data security measures to protect the Private Information they were required to provide.

178. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

Lack of Compensation

179. Defendant's Notice Letter fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and entirely fails to provide any redress for the unauthorized disclosure of Plaintiffs' and Class Members' Private Information, and the costs and time they now must spend attempting to mitigate their injuries.

180. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

181. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of fraud and identity theft.

182. Further, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

183. Specifically, victims suffered and will suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying fees for late or declined payments fees imposed for failed automatic payments tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

184. In addition, Plaintiffs and Class Members suffered a loss of value of their Private Information when it was acquired by cyberthieves in the Data Breach. Numerous courts have recognized the property of loss of value damages in related cases.

185. Plaintiffs and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to

the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

Injunctive Relief is Necessary to Protect Against Future Data Breaches.

186. Moreover, Plaintiffs and Class Members have an interest in ensuring that Private Information, which is believed to remain in Defendant's possession, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to employee training on cybersecurity awareness and prevention measures, storing data or documents containing Private Information so they are not accessible online, and ensuring that access to such data is password-protected.

187. Because of Defendant's failure to use reasonable measures to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, they suffered or are at a materially increased risk of imminently suffering

a. loss of control over how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

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

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

f. unauthorized use of their stolen Private Information; and

g. continued risk to their Private Information, which remains in Defendant's possession and is thus at risk for futures breaches so long as Defendant fails to take appropriate measures to protect it.

VI. CLASS ALLEGATIONS

188. Plaintiffs bring this nationwide class action individually and on behalf of all other persons similarly situated (the "Class") pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3).

189. Plaintiffs propose the following Class definition, subject to amendment based on information obtained through discovery:

> All individuals whose Private Information was compromised in Defendant's Data Breach beginning on or about February 29, 2024, as announced by Defendant, including all persons who received the Notice Letter from Defendant.

190. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

191. Plaintiffs reserve the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

192. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

193. This action satisfies the requirements for a class action under Rule 23(a)(1)-(3) and Rule 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

194. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The members of the Class are so numerous

that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Private Information of approximately 4,190 customers and/or employees of Defendant was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

195. **Commonality, Fed. R. Civ. P. 23(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. 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;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act and HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether hackers obtained Plaintiffs' and Class Members' Private Information in the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

h. Whether Defendant breached the covenant of good faith and fair dealing implied in its contracts with Plaintiffs and Class Members; and

i. Whether Plaintiffs and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

196. **Typicality, Fed. R. Civ. P. 23(a)(3):** The claims or defenses of Plaintiffs are typical of the claims or defenses of the proposed Class because Plaintiffs' claims are based upon the same legal theories and same violations of law. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

197. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating data breach class actions.

198. **Predominance, Fed. R. Civ. P. 23(b)(3):** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' Private Information was stored on the same computer systems and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

199. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many

reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions.

b. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

c. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

d. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

200. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Defendant's employees, the legal and factual issues are narrow and easily defined, and the Class Membership is limited. The Class does not contain so many persons that would make the

Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

201. In addition, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

202. 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 failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard customers' and employees' Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

203. Finally, all members of the proposed Class are readily ascertainable. Defendant

has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION
COUNT I: NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

204. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 203 above as if fully set forth herein.

205. Defendant required Plaintiffs and Class Members to submit private, confidential Private Information to Defendant as a condition of receiving products and services and/or employment from Defendant.

206. Plaintiffs and Class Members provided certain Private Information to Defendant including their names, Social Security numbers, dates of birth, medical equipment information, medical diagnosis and treatment information, health insurance information, and other personal information.

207. Defendant had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that Private Information.

208. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices by Defendant.

209. Plaintiffs and the Class Members had no ability to protect their Private Information in Defendant's possession.

210. By collecting and storing Plaintiffs' and Class Members' Private Information in its

computer systems, Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect if that Private Information was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

211. Defendant owed a duty of care to Plaintiffs and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

212. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its customers and/or its employees, which is recognized by laws and regulations including but not limited to the FTC Act, HIPAA, as well as the common law. Defendant was able to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach, yet it failed to.

213. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

214. Defendant's duty to use reasonable care in protecting Plaintiffs' and Class Members' confidential Private Information in its possession arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to reasonably protect such Private Information.

215. Defendant's duty also arose from its position as a healthcare provider. Defendant

holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Defendant, as a healthcare provider, was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members because of the Data Breach.

216. Defendant breached its duties, and was grossly negligent, by acts of omission or commission, by failing to use reasonable measures and indeed even minimally reasonable measures, to protect the Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' Private Information;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;

f. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

217. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Private Information would not have been compromised because Defendant would have identified the malicious activity and stopped the attack before the malicious actors had a chance to inventory Defendant's digital assets, stage them, and then exfiltrate them.

218. It was foreseeable that Defendant's failure to use reasonable measures to protect

Plaintiffs' and Class Members' Private Information would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

219. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would result in one or more types of injuries to them.

220. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

221. 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.

222. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

223. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide

adequate credit monitoring to all Class Members.

COUNT II: NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

224. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 203 above as if fully set forth herein.

225. Pursuant to the FTC Act, 15 U.S.C. § 45 *et seq.*, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

226. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

227. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, 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." *See* 45 C.F.R. § 164.304.

228. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

229. The injuries to Plaintiffs and Class Members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of the statutes described herein.

230. Plaintiffs and Class Members are within the class of persons the FTC Act and HIPAA were intended to protect.

231. The type of harm that resulted from the Data Breach was the type of harm the FTC Act and HIPAA were intended to guard against.

232. Defendant's failure to comply with the FTC Act and HIPAA and regulations constitutes negligence *per se.*

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

234. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

235. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

236. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

COUNT III: BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

237. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 203 above as if fully set forth herein.

238. Defendant required Plaintiffs and Class Members to provide and entrust their

Private Information as a condition of obtaining healthcare products and services and/or employment from Defendant.

239. When Plaintiffs and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiffs and Class Members if and when their Private Information was breached and compromised.

240. Specifically, Plaintiffs and Class Members entered into valid and enforceable implied contracts with Defendant when they agreed to provide their Private Information to Defendant.

241. The valid and enforceable implied contracts that Plaintiffs and Class Members entered into with Defendant included Defendant's promise to protect Private Information it collected from Plaintiffs and Class Members, or created on its own, from unauthorized disclosures. Plaintiffs and Class Members provided this Private Information in reliance on Defendant's promise.

242. Under the implied contracts, Defendant promised and was obligated to (a) provide products and services and/or employment to Plaintiffs and Class Members; and (b) protect Plaintiffs' and Class Members' Private Information (i) provided to obtain such services and/or (ii) created in connection therewith. In exchange, Plaintiffs and Class Members agreed to provide Defendant labor and/or payment to and their Private Information.

243. Both the provision of payment and/or employment, and the protection of Plaintiffs' and Class Members' Private Information, were material aspects of these implied contracts with Defendant.

244. Defendant's implied contracts for employment—contracts that include the

contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including Defendant's Notice of Privacy Practices and Employee Privacy Policy, as described *supra*.

245. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

246. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act and HIPAA.

247. Plaintiffs and Class Members who partnered or contracted with Defendant for products and services and/or employment and who provided their Private Information to Defendant, reasonably believed and expected that Defendant would adequately employ adequate data security to protect that Private Information. Defendant failed to do so.

248. A meeting of the minds occurred when Plaintiffs and the Class Members agreed to, and did, provide their Private Information to Defendant and agreed Defendant would receive labor and/or payment for, amongst other things, the protection of their Private Information.

249. Plaintiffs and Class Members performed their obligations under the contracts when they agreed Defendant would receive labor and/or payment and provided their Private Information to Defendant.

250. Defendant materially breached its contractual obligations to protect the Private Information it required Plaintiffs and Class Members to provide when it failed to implement even minimally reasonable logging and monitoring systems, among other safeguards, and thus allowed

Plaintiffs' and Class Members' data to be disclosed to criminal actors bent on identity theft, fraud, and extortion.

251. Defendant materially breached its contractual obligations to deal fairly and in good faith with Plaintiffs and Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

252. Defendant materially breached the terms of its implied contracts, including, but not limited to, by failing to comply with industry standards or the standards of conduct embodied in statutes like Section 5 of the FTC Act, or by failing to otherwise protect Plaintiffs' and Class Members' Private Information, as set forth *supra*.

253. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiffs and Class Members.

254. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains with Defendant, and instead received products and services and/or compensation for employment of a diminished value compared to that described in the implied contracts. Plaintiffs and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

255. Had Defendant disclosed that its data security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have contracted for employment with Defendant.

256. Plaintiffs and Class Members would not have provided and entrusted their Private Information to Defendant in the absence of the implied contracts between them and Defendant.

257. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

258. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely or adequate notice that their Private Information was compromised in and because of the Data Breach.

259. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members and the attendant Data Breach, Plaintiffs and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

260. Plaintiffs and Class Members, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

261. Plaintiffs and the Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members.

COUNT IV: BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Class)

262. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 203 above as if fully set forth herein.

263. At all times during Plaintiffs' and Class Members' interactions with Defendant and/or its agents, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Private Information it collected and maintained.

264. Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized parties.

265. Plaintiffs and Class Members provided their Private Information to Defendant and/or its agents with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

266. Plaintiffs and Class Members also provided their Private Information to Defendant and/or its agents with the explicit and implicit understandings that Defendant would take precautions to protect such Private Information from unauthorized disclosure.

267. Defendant voluntarily received in confidence Plaintiffs' and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

268. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security practices to secure Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

269. But for Defendant's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their sensitive and confidential Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Private Information, as well as their resulting damages.

270. As a direct and proximate result of Defendant's breaches of Plaintiffs' and Class

Members' confidence, Plaintiffs and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

271. The injuries and harm Plaintiffs and Class Members suffered were the reasonably foreseeable result of Defendant's breach of confidence and unauthorized disclosure of Plaintiffs' and Class Members' Private Information.

272. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

273. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

COUNT V: UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

274. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 203 above as if fully set forth herein.

275. This claim is pleaded in the alternative to the claim of breach of implied contract.

276. Plaintiffs and Class Members conferred direct benefits upon Defendant in the form of agreeing to provide their Private Information to Defendant, without which Defendant could not

perform the services it provides or pay its employees.

277. Defendant appreciated or knew of these benefits it received from Plaintiffs and Class Members. Under principles of equity and good conscience, Defendant should not be allowed to retain the full value of these benefits—specifically, the costs it saved by failing to implement reasonable or adequate data security practices with respect to the Private Information it collected from Plaintiffs and Class Members.

278. After all, Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information. And if such inadequacies were known, then Plaintiffs and Class Members would never have agreed to provide their Private Information, or payment or labor, to Defendant.

279. Defendant should be compelled to disgorge into a common fund, for the benefit of Plaintiffs and the Class, all funds that were unlawfully or inequitably gained despite Defendant's misconduct and the resulting Data Breach.

COUNT VI: INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

280. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 203 above as if fully set forth herein.

281. Plaintiffs and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to Defendant's protection of this Private Information in its possession against disclosure to unauthorized third parties.

282. Defendant owed a duty to its customers and employees, including Plaintiffs and Class Members, to keep their Private Information confidential and secure.

283. Defendant failed to protect Plaintiffs' and Class Members' Private Information and instead exposed it to unauthorized persons which is now publicly available, including through the publication of such information to the Dark Web where cybercriminals go to find their next identity

theft and extortion victims.

284. Defendant allowed unauthorized third parties access to and examination of the Private Information of Plaintiffs and Class Members, by way of Defendant's failure to protect the Private Information.

285. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and Class Members is highly offensive to a reasonable person and represents an intrusion upon Plaintiffs' seclusion as well as a public disclosure of private facts.

286. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their Private Information to Defendant as a condition of receiving healthcare products and services and/or employment, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

287. Subsequent to the intrusion, Defendant permitted Plaintiffs' and Class Members' data to be published online to countless cybercriminals whose mission is to misuse such information, including through identity theft and extortion.

288. Because Defendant had previously experienced a data breach, it was fully aware that a failure to implement industry standard cybersecurity safeguards was substantially certain to lead to the disclosure of Plaintiffs' and Class Members' sensitive Private Information.

289. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiffs' and Class Members' interests in solitude or seclusion, as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

290. Thus, Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate and insufficient.

291. Defendant acted with reckless disregard for Plaintiffs' and Class Members' privacy when it allowed improper access to its systems containing Plaintiffs' and Class Members' Private Information without protecting said data from the unauthorized disclosure, or even encrypting such information.

292. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' Private Information.

293. Because Defendant acted with this knowing state of mind, it had notice and knew of the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

294. As a direct and proximate result of Defendant's acts and omissions set forth above, Plaintiffs' and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer injuries and damages as set forth herein, including, without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

295. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

COUNT VII: BAILMENT
(On Behalf of Plaintiffs and the Class)

296. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 203 above as if fully set forth herein.

297. Plaintiffs and Class Members, on one hand, and Defendant, on the other, contemplated a mutual beneficial bailment when Plaintiffs and Class Members transmitted their Private Information to Defendant solely for the purpose of obtaining employment and/or medical products and services from Defendant.

298. Plaintiffs and Class Members entrusted their Private Information to Defendant for a specific purpose—to obtain employment and/or healthcare products and services—with an implied contract that the trust was to be faithfully executed, and the Private Information was to be accounted for when the special purpose was accomplished.

299. Defendant accepted Plaintiffs' and Class Members' Private Information for the specific purpose of obtaining employment or healthcare products and/or services from Defendant.

300. Defendant was duty-bound under the law to exercise ordinary care and diligence in safeguarding Plaintiffs' and Class Members' Private Information and to ensure through commercially reasonable and industry standard means that such data was not disclosed to cybercriminals. Indeed, Defendant's knew with substantial certainty the misuse beyond the stated

purpose that would occur without adequate protections.

301. Plaintiffs' and the Class Members' Private Information was used for a different purpose than Plaintiffs and Class Members intended, for a longer time period and/or in a different manner or place than Plaintiffs and Class Members intended.

302. As set forth in the preceding paragraphs, Plaintiffs and Class Members were damaged by Defendant's breach of the implied and understood terms of its bailment with Plaintiffs and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Shaun Ducrepin and Dulcie Walker, on behalf of themselves and all others similarly situated, pray for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding Plaintiffs and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

E. Awarding injunctive relief in the form of additional technical and administrative cybersecurity controls as is necessary to protect the interests of Plaintiffs and the Class;

F. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the transmitted Private Information;

G. Awarding attorneys' fees and costs, as allowed by law,

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

J. Any and all such relief to which Plaintiffs and the Class are entitled.

JURY TRIAL DEMAND

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: July 15, 2024

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (TN 23045)
Grayson Wells (TN 039658, MO 73068)
Andrew Mize, *pro hac vice*
STRANCH, JENNINGS & GARVEY PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
(615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com
amize@stranchlaw.com

Interim Lead Counsel

Certificate of Service

I hereby certify that a true and correct copy of the foregoing has been served via email via the CM/ECF system on all counsel of record on this 15th day of July, 2024, upon the following:

E. Todd Presnell
Kimberly Michelle Ingram-Hogan
Bradley Arant Boult Cummings LLP
1221 Broadway, Ste. 2400
Nashville, TN 37203
T: 615-252-2355
tpresnell@bradley.com
kingram@bradley.com

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV