IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CONNECTICUT

IN RE: YALE NEW HAVEN HEALTH SERVICES CORP. DATA BREACH LITIGATION.	Case No.: 3:25-cv-00609-SRU **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Jon Nathanson, Michael Liparulo, Amber Wilson, Stephen Quinn, Adam Snitkoff, Tyoka Brumfield, Julie Mott, as parent and guardian of J.D.R.A., a minor, Maria Krantz, as parent and guardian of F.R.K. and E.V.K., minors, Alexander Hudson, Nina Pallman, Lisa Taylor-Austin, Deb Brown, as parent and guardian of H.A.B., a minor, Trent Berger, Sarah Crowell, Eric Wilson, Erica Ortiz on behalf of herself and as parent and guardian of M.F. 1, M.F. 2, M.F. 3, and G.O.S., minors, Patricia Rodriguez, Robert Taylor, and Tiffany Adjei (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, bring this action against Defendant, Yale New Haven Health Services Corporation ("Yale" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE ACTION

1. This class action arises out of Defendant's failure to properly secure and safeguard the sensitive personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") of over **5.6 million** individuals.

2. Yale is a health system that includes "five acute-care hospitals, a medical foundation, several multispecialty centers and dozens of outpatient locations and ambulatory sites

stretching from Westchester County, New York, to Westerly, Rhode Island."[1]

3. Despite that Yale repeatedly processes and stores PII and PHI, Yale did not take adequate and reasonable precautions to safeguard this information. Defendant's data security failures allowed a targeted cyberattack to compromise Defendant's IT network ("Data Breach") that contained the Private Information of Plaintiffs and other individuals ("Class").

4. Specifically, on March 8, 2025, cyber criminals breached Defendant's inadequately protected IT network and ***stole*** Plaintiffs' and Class Members' Private Information.

5. The Private Information stolen by bad actors included names, dates of birth, addresses, telephone numbers, email addresses, individual's race or ethnicity, Social Security numbers, patient type, and medical record numbers.[2]

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted.

7. The mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant. Healthcare providers and health systems are frequently targets of data breaches because of the valuable information that they collect and store. Indeed, Yale's Chief Digital Health Officer, Lee Schwamm, recognized just last year that cybercriminals were increasingly becoming better at attacking health systems.[3] Thus, Defendant was on notice that failing to take appropriate steps to secure Private Information from those risks would make its patients' data a target for disclosure

[1] https://www.ynhhs.org/

[2] *See* https://www.ynhhs.org/news/yale-new-haven-health-notifies-patients-of-data-security-incident.

[3] *See* https://medcitynews.com/2024/06/cyberattack-ransomware-healthcare/.

and exploitation.

8. Defendant breached its duties and obligations by, at a minimum: (1) failing to design, implement, monitor, and maintain reasonable safeguards against foreseeable cybersecurity threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to encrypt or adequately encrypt the Private Information; and (4) otherwise failing to comply with HIPAA regulations and industry-standard data security practices.

9. Defendant impliedly understood its obligations and promised to safeguard Plaintiffs' and Class Members' Private Information. Plaintiffs and Class Members relied on these implied promises when seeking out and paying for Defendant's medical services. But for this mutual understanding, Plaintiffs and Class Members would not have provided Defendant with their Private Information. Defendant did not meet these reasonable expectations, causing Plaintiffs and Class Members to suffer injury.

10. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; and failing to take standard and reasonably available steps to prevent the Data Breach.

11. As a result of this conduct, Plaintiffs' and Class Members' Private Information that Defendant collected and maintained is now in the hands of data thieves. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung.

12. As a result of the Data Breach, Plaintiffs and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiffs and Class Members must now

and in the future closely monitor their accounts and online records to guard against identity theft and fraud. Such mitigation efforts include, and will continue to include in the future: (a) reviewing financial statements and credit reports; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

13. Plaintiffs and Class Members have suffered numerous, additional injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft and fraud; (d) loss of time incurred due to addressing actual identity theft; (e) deprivation of value of their Private Information; and (f) the continued risk to their sensitive Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it collected and maintained.

14. Through this Consolidated Complaint, Plaintiffs seek to remedy these harms on behalf of all similarly situated individuals whose Private Information was stolen during the Data Breach. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence and negligence *per se*, (ii) breach of implied contract, (iii) unjust enrichment, and (iv) declaratory relief.

15. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

PARTIES

16. Plaintiff Jon Nathanson is an adult individual who at all relevant times has been a citizen and resident of Fairfield, Connecticut.

17. Plaintiff Michael Liparulo is an adult individual who at all relevant times has been a citizen and resident of New London, Connecticut.

18. Plaintiff Amber Wilson is an adult individual who at all relevant times has been a citizen and resident of East Hartford, Connecticut.

19. Plaintiff Stephen Quinn is an adult individual who at all relevant times has been a citizen and resident of Shelton, Connecticut.

20. Plaintiff Adam Snitkoff is an adult individual who at all relevant times has been a citizen and resident of Fairfield, Connecticut.

21. Plaintiff Tyoka Brumfield is an adult individual who at all relevant times has been a citizen and resident of Waterbury, Connecticut.

22. Plaintiff Julie Mott, as parent and guardian of J.D.R.A., a minor, is an adult individual who at all relevant times has been a citizen and resident of Branford, Connecticut.

23. Plaintiff Maria Krantz, as parent and guardian of F.R.K. and E.V.K., minors, is an adult individual who at all relevant times has been a citizen and resident of Meriden, Connecticut.

24. Plaintiff Alexander Hudson is an adult individual who at all relevant times has been a citizen and resident of New Haven, Connecticut.

25. Plaintiff Nina Pallman is an adult individual who at all relevant times has been a citizen and resident of Coram, Connecticut.

26. Plaintiff Lisa Taylor-Austin is an adult individual who at all relevant times has been a citizen and resident of Milford, Connecticut.

27. Plaintiff Deb Brown, as parent and guardian of H.A.B., a minor, is an adult individual who at all relevant times has been a citizen and resident of Shelton, Connecticut.

28. Plaintiff Trent Berger is an adult individual who at all relevant times has been a citizen and resident of Clifton, Virginia.

29. Plaintiff Sarah Crowell is an adult individual who at all relevant times has been a citizen and resident of Eldon, Missouri.

30. Plaintiff Eric Wilson is an adult individual who at all relevant times has been a citizen and resident of Bridgeport, Connecticut.

31. Plaintiff Erica Ortiz, parent and guardian of M.F. 1, M.F. 2, M.F. 3, and G.O.S., minors, is an adult individual who at all relevant times has been a citizen and resident of West Haven, Connecticut.

32. Plaintiff Patricia Rodriguez is an adult individual who at all relevant times has been a citizen and resident of West Haven, Connecticut.

33. Robert Taylor is an adult individual who at all relevant times has been a citizen and resident of New London, Connecticut.

34. Plaintiff Tiffany Adjei is an adult individual who at all relevant times has been a citizen and resident of Derby, Connecticut.

35. Defendant is a healthcare provider and corporation organized under Connecticut law and with its principal place of business at 789 Howard Ave, New Haven, Connecticut 06519.

JURISDICTION AND VENUE

36. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100

class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Class Members are citizens of states that differ from Defendant.

37. This Court has personal jurisdiction over Defendant because Defendant conducts business in and has sufficient minimum contacts with Connecticut.

38. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and many of Defendant's acts complained of herein occurred within this District.

FACTUAL BACKGROUND

A. Defendant's Business

39. Defendant is a healthcare provider furnishing a wide variety of medical services to Connecticut patients.[4]

40. Plaintiffs and Class Members are current and former patients and/or parents of current or former patients of Defendant who received healthcare services from Defendant prior to March 2025.

41. As a condition and in exchange for receiving healthcare services from Defendant, Defendant's patients, including Plaintiffs and Class Members, were required to entrust Defendant with their and their minor children's highly sensitive Private Information.

42. In the course of collecting Private Information from Plaintiffs and Class Members, Defendant promised to provide adequate data security through its applicable privacy policy. For example, Defendant's Notice of Privacy Practices, provided to all patients receiving healthcare services from Defendant, promises and assurances as follows:

Our pledge to you:

[4] https://www.ynhhs.org/

> We understand that medical information about you is personal. We are committed to protecting medical information about you. We create a record of the care and services you receive to provide quality care and to comply with legal requirements. This notice applies to all of the records of your care generated by any of the separate facilities and providers described below. We are required by law to:
>
> - Keep medical information about you private;
> - Give you this notice of our legal duties and privacy practices with respect to medical information about you; and
> - Follow the terms of the notice that is currently in effect.[5]

43. Plaintiffs and Class Members relied on these promises from Defendant, a sophisticated business entity and healthcare provider, to implement reasonable practices to keep sensitive Private Information confidential and securely maintained, to use this information for necessary purposes only and make only authorized disclosures of this information, and to delete Private Information from Defendant's systems when no longer necessary for its legitimate business or healthcare purposes.

44. Unfortunately, Defendant failed to adhere to these promises and, as a result, Plaintiffs' and Class Members' Private Information was stolen in the Data Breach and has already been misused.

B. The Cyberattack and Data Breach

45. On March 11, 2025, Defendant posted a statement addressing IT services on its website.

[5] *See* https://www.ynhhs.org/policies

46. According to the statement, Defendant allegedly became aware of the Data Breach on March 8, 2025, after it noticed unusual activity affecting Defendant's Information Technology (IT) systems. Defendant launched an investigation and determined that an unauthorized third-party gained access to Defendant's network and, on March 8, 2025, stole Plaintiffs' and Class Members' Private Information.[6]

47. As a result of the Data Breach, cyber criminals were able to access and exfiltrate Plaintiffs' and Class Members' Private Information. The Private Information stolen in the Data Breach included Plaintiffs' and Class Members' demographic information (such as name, date of birth, address, telephone number, email address, race or ethnicity), Social Security number, patient type, and/or medical record number.[7]

48. The sensitive files exfiltrated in the Data Breach were stored in a way that left them unencrypted and vulnerable to access and exfiltration by unauthorized individuals.

49. Defendant had obligations created by contract, industry standards, common law, HIPAA regulations, the FTC Act, and its own promises and representations to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

50. Plaintiffs and Class Members provided their Private Information directly 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.

51. Through its "Notice of Data Security Incident" posted to Defendant's website, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach

[6] https://www.ynhhs.org/legal-notices
[7] *Id*.

and accordingly encouraged breach victims to take steps to mitigate their risk of identity theft, such as reviewing statements they receive from their healthcare providers and to immediately report any inaccuracies to the provider.[8]

52. Defendant offered abbreviated, non-automatic credit monitoring services to victims. While this acknowledges (and is an admission of) the harm posed to Plaintiffs and Class Members as a result of the Data Breach, it does not adequately address the lifelong harm that victims face following the Data Breach. Unfortunately, the credit monitoring and identity theft protection services are only offered to individuals whose Social Security numbers were stolen in the Data Breach, though no information or documents were provided by Defendant confirming how it determined whose Social Security numbers were stolen.

53. As a result of the Data Breach, Plaintiffs and Class Members are at a substantial and imminent risk of identity theft because their sensitive Private Information (including their Social Security numbers) was ***stolen*** in a targeted Data Breach. Further, Plaintiffs and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

54. The unencrypted Private Information of Plaintiffs and Class Members will likely end up for sale (or already is for sale) on the dark web as that is the *modus operandi* of hackers. This is especially true in this case where Plaintiffs' and Class Members' Social Security numbers were stolen. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of

[8] *Id*.

Plaintiffs and Class Members. In turn, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

C. Defendant Knew the Risks of Storing Valuable Private Information and the Foreseeable Harm to Victims.

55. At all relevant times, Defendant knew it was storing valuable and confidential Private Information on its systems and servers and that it would, therefore, be an attractive target for cybercriminals.

56. Defendant also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was stolen, as well as intrusion into their highly private health information.

57. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others. Therefore, it was foreseeable that Defendant could and would suffer a data breach if it did not adequately protect Plaintiffs' and Class Members' Private Information.

58. Further, Defendant was keenly aware that its servers were a target for a data breach as it acknowledged in its "Notices of Privacy Practices" that "[w]e understand that medical information about you is personal. We are committed to protecting medical information about you."[9]

59. In fact, in 2024 alone, there were 2,850 data breaches and 3,158 total data compromises.[10] Further, the healthcare industry was the second highest industry that suffered data compromises in 2024.[11] In the last 24 months alone, 797 data breaches of healthcare organizations

[9] *See* https://www.ynhhs.org/policies
[10] https://www.idtheftcenter.org/publication/2024-data-breach-report/
[11] *Id.*

and their business associates were reported to the U.S. Department of Health and Human Services Office for Civil Rights Breach Portal, including Yale New Haven Health System reporting on April 11, 2025 a breach of its network server affecting 5,556,702 patients.[12] Therefore, it was certainly foreseeable that Defendant's failure to adequately protect Plaintiffs' and Class Members' Private Information would result in the Data Breach.

60. The Private Information stolen in the Data Breach has considerable value and constitutes an enticing and well-known target to hackers. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13]

61. Moreover, Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors

[12] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[13] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

> demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

62. 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.

63. Further, hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[15] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

64. With respect to Data Breaches implicating PHI, a study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[16]

65. 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."[17]

---

[14] Social Security Administration, Identity Theft and Your Social Security Number, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf

[15] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/

[16] https://distilgovhealth.com/2019/10/03/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud/

[17] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon

66. Health information in particular is likely to be used in detrimental ways—such as by leveraging sensitive personal health details and diagnoses to extort or coerce someone, or through serious and long-term identity theft.[18]

67. Plaintiffs and the Class Members have been injured by Defendant's unauthorized disclosure of their confidential and private medical records and PHI.

68. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S.

69. The breadth of data stolen in the Data Breach, including Social Security numbers and medical records, makes the information particularly valuable to cyber criminals and leaves Defendant's current and former patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

70. 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."[19] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[20]

---

[18] *Id.*

[19] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat

[20] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com/gx/en/consulting-

71. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[21]

72. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can **sell for up to $1,000 online.**"[22]

73. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[23]

---

services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

[21] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/

[22] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon

[23] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf

74. Even if stolen Private Information does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained Private Information about the individual, such as names, addresses, email addresses, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

D. Defendant Breached its Duty to Protect its Patients' Private Information.

75. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members.

76. Indeed, it appears that Yale's decision ***not*** to adequately secure its IT systems was a calculated decision. According to Yale's Chief Digital Health Officer, there is a "trade-off" between "security and productivity." Specifically, the more Yale "ramp[ed] down the access and close[s] down [its] networks to keep them secure, the harder it is for workers to access what they need to get the work done[.]"[24]

77. Moreover, Defendant could have destroyed the data that it collected or moved it to a much safer and less-accessible place, especially for individuals with whom it had not had a relationship for a long period of time or who had ended their relationship with Yale. It is clear Yale did not do so. According to Yale's own records, the number of individuals impacted by the breach ***far exceeds*** the approximate number of patients Yale treats each year.[25] This confirms that Yale

[24] https://medcitynews.com/2024/06/cyberattack-ransomware-healthcare/
[25] https://www.ynhhs.org/about/corporate-overview/system-statistics#:~:text=Yale%20New%20Haven%20Health%20includes,Employees:%2029%2C486

retained records in its compromised IT system for much longer than it should have, and that it should have implemented the reasonable process of deleting unnecessary records.

78. Additionally, Defendant could have encrypted the information to prevent bad actors from being able to use the information for malicious purposes if they were able to breach its system. That Yale's Data Breach Notice makes no mention of encryption, and offers only credit monitoring, strongly suggests this data was not encrypted and was stored in plain text that was readable to cybercriminals.[26]

79. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

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

Defendant Failed to Comply with the FTC Act and the HIPAA Regulations

81. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA"). Under

[26] *Cf.* Notice of Data Breach, Byte Federal Inc. (Dec. 13, 2024) ("The data was encrypted, but the attacker also acquired the encryption key."), *available at* https://mm.nh.gov/files/uploads/doj/remote-docs/byte-federal-20241213.pdf; Notice of Data Breach, Blink Mobility (Jan. 8, 2024) ("Although the exposed password data was encrypted it is recommended that all customers update the password on any applications that share the same password as the legacy Blink Mobility app."), *available at* https://oag.ca.gov/system/files/Notice%20of%20Breach_Blink%20Mobility.pdf.

state and federal law, businesses like Defendant have duties to protect patients' Private Information and to notify them about breaches.

82. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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.

83. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal consumer 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]

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

85. 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 all networks for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

---

[27] *Protecting Personal Information: A Guide for Business, Federal Trade Commission* (2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[28] *Id*.

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

87. These FTC enforcement actions include actions against technology service institutions, like Defendant.

88. 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 PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

89. As described herein, Defendant failed to properly implement basic data security practices.

90. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

91. Further, Defendant was required but failed to comply with HIPAA rules and regulations.

92. Defendant is a covered business 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.

93. 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.

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

95. 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.

96. 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.

97. 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).

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

99. 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).

100. 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).

101. 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." US Department of Health & Human Services, Security Rule Guidance

Material.[29] 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.[30]

102. As alleged in this Consolidated 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 PHI.

Defendant Failed to Comply with the Connecticut Data Privacy Act ("CTDPA") and the CTDPA's Health Data Provisions

103. The Connecticut Data Privacy Act ("CTDPA") requires companies that process a certain amount of consumer personal data employ reasonable cybersecurity practices to prevent unauthorized access or theft. CGA § 42-515, *et seq.* All entities with operations in Connecticut that collect consumer health data are covered by CTDPA, including Defendant.

104. While CTDPA does not explicitly require a covered entity to use encryption to safeguard personal data, using encryption is generally considered a reasonable data practice when storing and transmitting personal data.[31] Defendant's failure to encrypt Plaintiffs' and the Class's data—or to use other effective cybersecurity measures—was a violation of the standards set out in the CTDPA.

---

[29] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
[30] *Id*.
[31] Matthew Hoppler, *Encryption of Personal Data by Financial Institutions and Utilities in Connecticut and Neighboring States*, Conn. Office of Legislative Research (Mar. 5, 2024), *available at* https://www.cga.ct.gov/2024/rpt/pdf/2024-R-0049.pdf ("While CTDPA does not explicitly require a covered entity to use encryption to safeguard personal data, using encryption is generally considered a reasonable data practice when storing and transmitting personal data.").

105. CTDPA also contains heightened requirements related to entities that collect PHI. Defendant's failure to establish reasonable security measures, given the nature of the information it stores, also violated these heightened standards.

106. Accordingly, Defendant failed to comply with the CTDPA and the Health Data Provisions of the CTDPA.

E. Plaintiffs and Class Members Suffered Damages.

107. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. As a result of the Data Breach, Plaintiffs and Class Members must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) 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 (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

108. Once Private Information is stolen, there is virtually no way to ensure that the stolen 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. Further, the value of Plaintiffs' and Class Members' Private Information has been diminished by its theft in the Data Breach.

109. As a result of the Data Breach, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or further misuse of their Private Information.

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

COMMON INJURIES AND DAMAGES

111. As result of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

112. Due to the Data Breach, 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) theft of their Private Information; (b) the substantial and imminent risk of identity theft; (c) invasion of privacy; (d) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (e) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (f) "out of pocket" costs incurred due to actual identity theft; (g) loss of time incurred due to actual identity theft and the substantial and imminent risk of identity theft; (h) loss of time due to increased spam and targeted marketing emails; (i) the loss of benefit of the bargain; (j) diminution in value of their Private Information; and (k) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

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

113. 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.

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

115. 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.

116. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[32] 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

[32] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-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.[33] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

117. 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.[34] 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.[35] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[36]

118. For example, as discussed above, Social Security numbers 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. Further, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security

---

[33] *Id.*

[34] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

[35] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[36] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

number without significant paperwork and evidence of actual misuse.

119. Even then, a 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."[37]

120. 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 being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[38]

121. Finally, armed with an individual's Social Security number, scammers can specifically use the Social Security numbers to commit credit card fraud.[39] Therefore, considering the Private Information stolen in the Data Breach includes Social Security numbers, Plaintiffs' and Class Members' identity theft and fraud occurring after the Data Breach is fairly traceable to the Data Breach.

122. Next, as discussed above, theft of PHI, in particular, is gravely serious: "A thief

---

[37] 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.

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

[39] *See*, *e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can- do-with-your-social-security-number-108597.

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."[40]

123. One such example of criminals using PHI for profit is the development of "Fullz" packages. Cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

124. The development of "Fullz" packages means that stolen PHI 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 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 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 fairly traceable to the Data Breach.

125. 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.[41]

---

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

[41] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

126. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[42] Defendant did not rapidly report to Plaintiffs and the Class that their Private Information had been stolen. Even worse, Defendant has not even provided Plaintiffs and Class Members with individualized notice of the Data Breach.

127. 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.

128. 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.

129. 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.

130. Therefore, the risk of identity theft to Plaintiffs and Class Members is substantial and imminent because: (i) Plaintiffs' and Class Members' Private Information was targeted in cyberattack and stolen in the Data Breach; and (ii) the Private Information stolen in the Data Breach is sensitive and can be used to commit identity theft and fraud.

---

[42] *Id.*

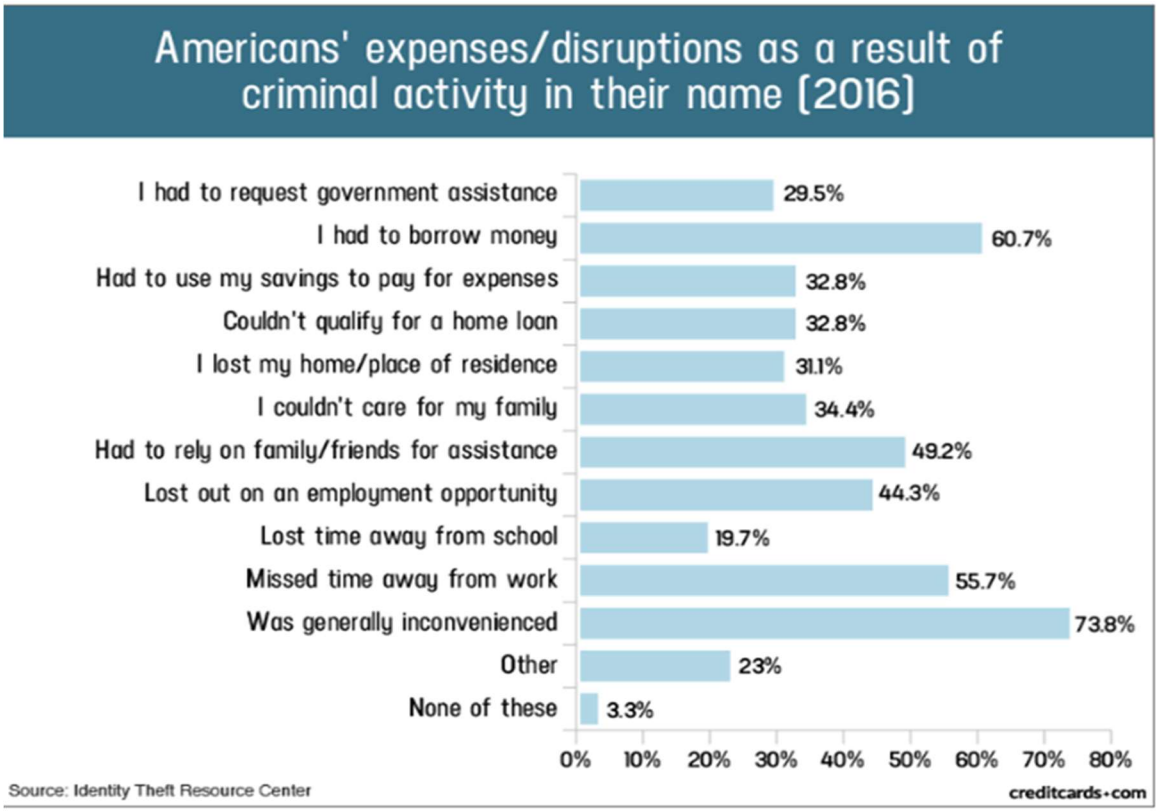
B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

131. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was stolen, 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 resource and asset of time has been lost.

132. 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 to remedy fraudulent transactions to their accounts, 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.

133. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[43]

[43] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



134. In the event that Plaintiffs and Class Members experience additional instances of 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."[44] 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 7 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

[44] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

correcting their credit reports.[45]

135. Defendant even recognizes the need for Plaintiffs and Class Members to spend such time mitigating the harmful effects of the Data Breach by suggesting that Plaintiffs and Class Members: (i) enroll in credit monitoring, (ii) change passwords and security questions, (iii) monitor financial accounts and credit reports, and (iv) carefully review any unanticipated emails, text messages, chats, or voicemails.

136. Nonetheless, time spent mitigating the harmful effects of the Data Breach is reasonable and necessary because: (i) Plaintiffs' and Class Members' Private Information was targeted in cyberattack and stolen in the Data Breach; (ii) the Private Information stolen in the Data Breach is sensitive and can be used to commit identity theft and fraud; and (iii) multiple Plaintiffs have already suffered actual misuse of their Private Information in the form of identity theft and fraud.

C. Diminution in Value of the Private Information

137. PII and PHI are valuable property rights.[46] Their value is axiomatic, especially considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

138. 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

[45] *See* https://www.identitytheft.gov/Steps

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

the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

139. Private Information can sell for as much as $363 per record according to the Infosec Institute.[47]

140. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data was selling on the dark web for $50 and up.[48]

141. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[49] 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.[50, 51] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[52]

142. 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 and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

---

[47] *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.

[48] *See* https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

[49] *See* https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[50] *See* https://datacoup.com.

[51] *See* https://digi.me/what-is-digime.

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

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

143. To date, Defendant has done **nothing** to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant places the burden on remedying the Data Breach completely on the Plaintiffs and Class Members.

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

145. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his 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.

146. Furthermore, the information accessed and stolen 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.[53] The information stolen in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

147. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of

[53] *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

fraud and identity theft for many years into the future.

148. 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.

E. Loss of Benefit of the Bargain

149. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to provide their Private Information, which was a condition precedent to obtain medical services, Plaintiffs, as consumers and patients, understand and expect that they were, in part, paying for data security to protect the Private Information required to be collected from them.

150. 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.

F. Injunctive Relief is Necessary to Protect Against Future Data Breaches

151. Plaintiffs and Class Members have an interest in ensuring that Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

152. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages and actual misuse of their Private

Information. These damages include, but are not limited to: (a) actual misuse of their Private Information; (b) theft of their Private Information; (c) the substantial and imminent risk of identity theft; (d) invasion of privacy; (e) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (f) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (g) "out of pocket" costs incurred due to actual identity theft; (h) loss of time incurred due to actual identity theft and the substantial and imminent risk of identity theft; (i) loss of time due to increased spam and targeted marketing emails; (j) the loss of benefit of the bargain; (k) diminution in value of their Private Information; and (l) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

PLAINTIFF JON NATHANSON'S EXPERIENCE

153. Plaintiff Jon Nathanson ("Plaintiff Nathanson") entrusted his Private Information to Defendant as a patient of Defendant.

154. Plaintiff Nathanson's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

155. Plaintiff Nathanson received a Data Breach notification letter from Defendant stating that his Private Information was involved in the Data Breach.

156. Plaintiff Nathanson is very careful about sharing his sensitive information.

157. Plaintiff Nathanson stores any documents containing his Private Information in a safe and secure location.

158. Because of the Data Breach, Plaintiff Nathanson's Private Information is now in the hands of cybercriminals.

159. Plaintiff Nathanson has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

160. As a result of the Data Breach, which exposed his highly valuable Private Information, Plaintiff Nathanson is now imminently at risk of crippling future identity theft and fraud.

161. As a result of the Data Breach, Plaintiff Nathanson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Nathanson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, responding to and blocking spam calls and text messages, changing his sensitive information, researching ways to mitigate the harmful effects of the Data Breach, and taking other protective and ameliorative steps in response to the Data Breach.

162. As a result of the Data Breach, Plaintiff Nathanson has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Nathanson fears that criminals will use his information to commit additional instances of identity theft.

163. Plaintiff Nathanson has already spent considerable time and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

164. Plaintiff Nathanson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Nathanson's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Nathanson's Private Information; and (e) continued risk to Plaintiff Nathanson's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF MICHAEL LIPARULO'S EXPERIENCE

165. Plaintiff Michael Liparulo ("Plaintiff Liparulo") entrusted his Private Information to Defendant as a patient of Defendant.

166. Plaintiff Liparulo's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

167. Plaintiff Liparulo received a Data Breach notification letter from Defendant stating that his Private Information was involved in the Data Breach.

168. Plaintiff Liparulo is very careful about sharing his sensitive information.

169. Plaintiff Liparulo stores any documents containing his Private Information in a safe and secure location.

170. Because of the Data Breach, Plaintiff Liparulo's Private Information is now in the hands of cybercriminals.

171. Plaintiff Liparulo has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

172. As a result of the Data Breach, which exposed his highly valuable Private Information, Plaintiff Liparulo is now imminently at risk of crippling future identity theft and fraud.

173. As a result of the Data Breach, Plaintiff Liparulo has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Liparulo has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

174. As a result of the Data Breach, Plaintiff Liparulo has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Liparulo fears that criminals will use his information to commit additional instances of identity theft.

175. Plaintiff Liparulo has already spent considerable time and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

176. Plaintiff Liparulo has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Liparulo's

Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Liparulo's Private Information; and (e) continued risk to Plaintiff Liparulo's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF AMBER WILSON'S EXPERIENCE

177. Plaintiff Amber Wilson ("Plaintiff Wilson") entrusted her Private Information to Defendant as a patient of Defendant.

178. Plaintiff Wilson's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

179. Plaintiff Wilson received a Data Breach notification letter from Defendant stating that her Private Information was involved in the Data Breach.

180. Plaintiff Wilson is very careful about sharing her sensitive information.

181. Plaintiff Wilson stores any documents containing her Private Information in a safe and secure location. Plaintiff Wilson has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

182. Because of the Data Breach, Plaintiff Wilson's Private Information is now in the hands of cybercriminals and on the dark web and has already been misused. Indeed, the payment

card Plaintiff Wilson used to pay for Defendant's medical services was fraudulently used soon after the Data Breach occurred.

183. Plaintiff Wilson has also suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

184. As a result of the Data Breach, which exposed her highly valuable Private Information, and in light of the fraud she has already experienced, Plaintiff Wilson is now imminently at risk of crippling future identity theft and fraud.

185. As a result of the Data Breach, Plaintiff Wilson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Wilson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her account statements and other information, paying for credit monitoring services as a result of Defendant's failure to provide a free credit monitoring service following the Data Breach, responding to and blocking spam calls and text messages, and taking other protective and ameliorative steps in response to the Data Breach.

186. As a result of the Data Breach, Plaintiff Wilson has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Wilson fears that criminals will use her information to commit identity theft.

187. Plaintiff Wilson has already spent considerable time and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

188. Plaintiff Wilson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Wilson's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Wilson's Private Information; and (e) continued risk to Plaintiff Wilson's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF STEPHEN QUINN'S EXPERIENCE

189. Plaintiff Stephen Quinn ("Plaintiff Quinn") entrusted his Private Information to Defendant as a patient of Defendant.

190. Plaintiff Quinn's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

191. Plaintiff Quinn received a Data Breach notification letter from Defendant stating that his Private Information was involved in the Data Breach.

192. Plaintiff Quinn is very careful about sharing his sensitive information.

193. Plaintiff Quinn stores any documents containing his Private Information in a safe and secure location. Plaintiff Quinn has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

194. Because of the Data Breach, Plaintiff Quinn's Private Information is now in the hands of cybercriminals and on the dark web.

195. Plaintiff Quinn has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

196. As a result of the Data Breach, which exposed his highly valuable Private Information, Plaintiff Quinn is now imminently at risk of crippling future identity theft and fraud.

197. As a result of the Data Breach, Plaintiff Quinn has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Quinn has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, freezing his credit, enrolling in credit monitoring services, responding to and blocking spam calls and text messages, and taking other protective and ameliorative steps in response to the Data Breach.

198. As a result of the Data Breach, Plaintiff Quinn has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Quinn fears that criminals will use his information to commit identity theft.

199. Plaintiff Quinn has already spent considerable time and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

200. Plaintiff Quinn has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Quinn's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Quinn's Private Information; and (e) continued risk to Plaintiff Quinn's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF ADAM SNITKOFF'S EXPERIENCE

201. Plaintiff Adam Snitkoff ("Plaintiff Snitkoff") is a longtime patient of Defendant, and as a patient, he entrusted his Private Information to Defendant which included his name, address, driver's license number, and Social Security number.

202. Plaintiff Snitkoff's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

203. Plaintiff Snitkoff received a Data Breach notification letter from Defendant stating that his Private Information was involved in the Data Breach.

204. Plaintiff Snitkoff is very careful about sharing his sensitive information.

205. Plaintiff Snitkoff stores any documents containing his Private Information in a safe and secure location.

206. Because of the Data Breach, Plaintiff Snitkoff's Private Information is now in the hands of cybercriminals, and, since April 2025, he has been bombarded with more spam calls and texts than he's ever experienced before.

207. Plaintiff Snitkoff has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy— including a new suspicious medical bill for a charge that he does not recognize. This suspicious bill will now require Plaintiff Snitkoff to spend additional time, and possibly money, to resolve.

208. As a result of the Data Breach, which exposed his highly valuable Private Information, Plaintiff Snitkoff is now imminently at risk of crippling future identity theft and fraud.

209. As a result of the Data Breach, Plaintiff Snitkoff has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Plaintiff Snitkoff is now highly vigilant and has already expended significant time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, reviewing his credit report information sometimes on a daily basis, changing his passwords, , contacting his bank to change his account information, installing a new router and changing his IP address, responding to and blocking spam calls and text messages, and taking other protective and ameliorative steps in response to the Data Breach.

210. As a result of the Data Breach, Plaintiff Snitkoff has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing

and misusing his Private Information. Plaintiff Snitkoff fears that criminals will use his information to commit identity theft.

211. Moreover, Plaintiff Snitkoff's wife and children are also patients of Defendant, and he is worried that their data was also exposed and that they have not been made aware of the risks to their Private Information because they did not receive notice letters from Defendant.

212. Plaintiff Snitkoff has already spent considerable time and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

213. Plaintiff Snitkoff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Snitkoff's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Snitkoff's Private Information; and (e) continued risk to Plaintiff Snitkoff's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF TYOKA BRUMFIELD'S EXPERIENCE

214. Plaintiff Tyoka Brumfield ("Plaintiff Brumfield") entrusted her Private Information to Defendant as a patient of Defendant.

215. Plaintiff Brumfield's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

216. Plaintiff Brumfield received a Data Breach notification letter from Defendant stating that her Private Information was involved in the Data Breach.

217. Plaintiff Brumfield is very careful about sharing her sensitive information.

218. Plaintiff Brumfield stores any documents containing her Private Information in a safe and secure location.

219. Because of the Data Breach, Plaintiff Brumfield's Private Information is now in the hands of cybercriminals and on the dark web.

220. Plaintiff Brumfield has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

221. As a result of the Data Breach, which exposed her highly valuable Private Information, Plaintiff Brumfield is now imminently at risk of crippling future identity theft and fraud.

222. As a result of the Data Breach, Plaintiff Brumfield has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Brumfield has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including thoroughly reviewing her account statements and other information and taking other protective and ameliorative steps in response to the Data Breach.

223. As a result of the Data Breach, Plaintiff Brumfield has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Brumfield fears that criminals will use her information to commit identity theft.

224. Plaintiff Brumfield has already spent considerable time and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

225. Plaintiff Brumfield has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Brumfield's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Brumfield's Private Information; and (e) continued risk to Plaintiff Brumfield's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF JULIE MOTT'S EXPERIENCE

226. Plaintiff Julie Mott ("Plaintiff Mott") entrusted her minor child's Private Information to Defendant as a patient of Defendant.

227. Plaintiff Mott's minor child's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

228. Plaintiff Mott received a Data Breach notification letter from Defendant stating that her minor child's Private Information was involved in the Data Breach.

229. Plaintiff Mott is very careful about sharing the sensitive information of her minor child.

230. Plaintiff Mott stores any documents containing her minor child's Private Information in a safe and secure location.

231. Because of the Data Breach, Plaintiff Mott's minor child's Private Information is now in the hands of cybercriminals and on the dark web.

232. Plaintiff Mott's minor child has suffered actual injury from the exposure and theft of their Private Information—which violates their right to privacy.

233. As a result of the Data Breach, which exposed highly valuable Private Information, Plaintiff Mott's minor child is now imminently at risk of crippling future identity theft and fraud.

234. As a result of the Data Breach, Plaintiff Mott has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Mott has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her minor child's account and provider statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

235. As a result of the Data Breach, Plaintiff Mott has experienced stress, anxiety, and concern due to the loss of her minor child's privacy and concern over the impact of cybercriminals accessing and misusing her minor child's Private Information. Plaintiff Mott fears that criminals will use such information to commit identity theft.

236. Plaintiff Mott has already spent considerable time and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

237. Plaintiff Mott has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's minor child's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Mott's minor child's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Mott's minor child's Private Information; and (e) continued risk to Plaintiff Mott's minor child's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF MARIA KRANTZ'S EXPERIENCE

238. Plaintiff Maria Krantz ("Plaintiff Krantz") entrusted her minor children's Private Information to Defendant as patients of Defendant.

239. Plaintiff Krantz's minor children's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

240. Plaintiff Krantz received a Data Breach notification letter from Defendant stating that her minor children's Private Information was involved in the Data Breach.

241. Plaintiff Krantz is very careful about sharing the sensitive information of her minor children.

242. Plaintiff Krantz stores any documents containing her minor children's Private Information in a safe and secure location.

243. Because of the Data Breach, Plaintiff Krantz's minor children's Private Information is now in the hands of cybercriminals and on the dark web.

244. Plaintiff Krantz's minor children have suffered actual injury from the exposure and theft of their Private Information—which violates their right to privacy.

245. As a result of the Data Breach, which exposed highly valuable Private Information, Plaintiff Krantz's minor children are now imminently at risk of crippling future identity theft and fraud.

246. As a result of the Data Breach, Plaintiff Krantz has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Krantz has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her minor children's account and provider statements

and other information, and taking other protective and ameliorative steps in response to the Data Breach.

247. As a result of the Data Breach, Plaintiff Krantz has experienced stress, anxiety, and concern due to the loss of her minor children's privacy and concern over the impact of cybercriminals accessing and misusing her minor children's Private Information. Plaintiff Krantz fears that criminals will use such information to commit identity theft.

248. Plaintiff Krantz has already spent considerable time and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

249. Plaintiff Krantz has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's minor child's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Krantz's minor child's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Krantz's minor children's Private Information; and (e) continued risk to Plaintiff Krantz's minor children's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF ALEXANDER HUDSON'S EXPERIENCE

250. Plaintiff Alexander Hudson ("Plaintiff Hudson") entrusted his Private Information to Defendant as a patient of Defendant.

251. Plaintiff Hudson's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

252. Plaintiff Hudson received a Data Breach notification letter from Defendant stating that his Private Information was involved in the Data Breach.

253. Plaintiff Hudson is very careful about sharing his sensitive information.

254. Plaintiff Hudson stores any documents containing his Private Information in a safe and secure location.

255. Because of the Data Breach, Plaintiff Hudson's Private Information is now in the hands of cybercriminals and on the dark web.

256. Plaintiff Hudson has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy. Plaintiff Hudson additionally experienced unrecognized charges on his payment card since February 2025, as well as an increase in spam calls and texts. Plaintiff Hudson experienced two fraudulent charges on his American Express credit card for $1,000 each.

257. As a result of the Data Breach, which exposed his highly valuable Private Information, Plaintiff Hudson is now imminently at risk of crippling future identity theft and fraud.

258. As a result of the Data Breach, Plaintiff Hudson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Hudson has already expended

time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, responding to and blocking spam calls and text messages, and taking other protective and ameliorative steps in response to the Data Breach.

259. As a result of the Data Breach, Plaintiff Hudson has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Hudson fears that criminals will use his information to commit identity theft.

260. Plaintiff Hudson has already spent considerable time and money and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

261. Plaintiff Hudson has also suffered injury directly and proximately caused by the Data Breach, including: (a) fraud; (b) theft of Plaintiff's valuable Private Information; (c) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Hudson's Private Information being placed in the hands of cybercriminals; (d) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (e) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Hudson's Private Information; and (f) continued risk to Plaintiff Hudson's Private Information, which remains in the possession of Defendant and which is subject to further breaches

so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF NINA PALLMAN'S EXPERIENCE

262. Plaintiff Nina Pallman ("Plaintiff Pallman") entrusted her Private Information to Defendant as a patient of Defendant.

263. Plaintiff Pallman's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

264. Plaintiff Pallman received a Data Breach notification letter from Defendant stating that her Private Information was involved in the Data Breach.

265. Plaintiff Pallman is very careful about sharing her sensitive information.

266. Plaintiff Pallman stores any documents containing her Private Information in a safe and secure location.

267. Because of the Data Breach, Plaintiff Pallman's Private Information is now in the hands of cybercriminals and on the dark web.

268. Plaintiff Pallman has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy. Plaintiff Pallman has additionally experienced an increase in spam calls and texts.

269. As a result of the Data Breach, which exposed her highly valuable Private Information, Plaintiff Pallman is now imminently at risk of crippling future identity theft and fraud.

270. As a result of the Data Breach, Plaintiff Pallman has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Pallman has already expended

time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her account statements and other information, responding to and blocking spam calls and text messages, and taking other protective and ameliorative steps in response to the Data Breach.

271. As a result of the Data Breach, Pallman has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Pallman fears that criminals will use her information to commit identity theft.

272. Plaintiff Pallman has already spent considerable time and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

273. Plaintiff Pallman has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Pallman's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Pallman's Private Information; and (e) continued risk to Plaintiff Pallman's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF LISA TAYLOR-AUSTIN'S EXPERIENCE

274. Plaintiff Lisa Taylor-Austin ("Plaintiff Taylor-Austin") entrusted her Private Information to Defendant as a patient of Defendant.

275. Plaintiff Taylor-Austin's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

276. Plaintiff Taylor-Austin received a Data Breach notification letter from Defendant stating that her Private Information was involved in the Data Breach.

277. Plaintiff Taylor-Austin is very careful about sharing her sensitive information.

278. Plaintiff Taylor-Austin stores any documents containing her Private Information in a safe and secure location. Plaintiff Taylor-Austin has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

279. Because of the Data Breach, Plaintiff Taylor-Austin's Private Information is now in the hands of cybercriminals and on the dark web.

280. Plaintiff Taylor-Austin has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy. Plaintiff Taylor-Austin has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy. Plaintiff Taylor-Austin additionally experienced unrecognized charges on her payment card since February 2025, as well as an increase in spam calls and texts. Plaintiff Taylor-Austin experienced fraudulent charges on her payment card made to Avis Car Rental for approximately $1,000.

281. As a result of the Data Breach, which exposed her highly valuable Private Information, Plaintiff Taylor-Austin is now imminently at risk of crippling future identity theft and fraud.

282. As a result of the Data Breach, Plaintiff Taylor-Austin has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Taylor-Austin has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her account statements and other information, enrolling in credit monitoring services, responding to and blocking spam calls and text messages, and taking other protective and ameliorative steps in response to the Data Breach.

283. As a result of the Data Breach, Plaintiff Taylor-Austin has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Taylor-Austin fears that criminals will use her information to commit identity theft.

284. Plaintiff Taylor-Austin has already spent considerable time and money, including the purchase of Aura credit monitoring protection, and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

285. Plaintiff Taylor-Austin has also suffered injury directly and proximately caused by the Data Breach, including: (a) fraud; (b) theft of Plaintiff's valuable Private Information; (c) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Taylor-Austin's Private Information being placed in the hands of cybercriminals; (d) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (e)

damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Taylor-Austin's Private Information; and (f) continued risk to Plaintiff Taylor-Austin's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF DEB BROWN'S EXPERIENCE

286. Plaintiff Deb Brown ("Plaintiff Brown") entrusted her minor child's Private Information to Defendant as a patient of Defendant.

287. Plaintiff Brown's minor child's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

288. Plaintiff Brown received a Data Breach notification letter from Defendant stating that her minor child's Private Information was involved in the Data Breach.

289. Plaintiff Brown is very careful about sharing the sensitive information of her minor child.

290. Plaintiff Brown stores any documents containing her minor child's Private Information in a safe and secure location.

291. Because of the Data Breach, Plaintiff Brown's minor child's Private Information is now in the hands of cybercriminals and on the dark web.

292. Plaintiff Brown's minor child has suffered actual injury from the exposure and theft of their Private Information—which violates their right to privacy.

293. As a result of the Data Breach, which exposed highly valuable Private Information, Plaintiff Brown's minor child is now imminently at risk of crippling future identity theft and fraud.

294. As a result of the Data Breach, Plaintiff Brown has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Brown has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her minor child's account and provider statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

295. As a result of the Data Breach, Plaintiff Brown has experienced stress, anxiety, and concern due to the loss of her minor child's privacy and concern over the impact of cybercriminals accessing and misusing her minor child's Private Information. Plaintiff Brown fears that criminals will use such information to commit identity theft.

296. Plaintiff Brown has already spent considerable time and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

297. Plaintiff Brown has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's minor child's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Brown's minor child's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's

defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Brown's minor child's Private Information; and (e) continued risk to Plaintiff Brown's minor child's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF TRENT BERGER'S EXPERIENCE

298. Plaintiff Trent Berger ("Plaintiff Berger") entrusted his Private Information to Defendant as a patient of Defendant.

299. Plaintiff Berger's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

300. Plaintiff Berger received a Data Breach notification letter from Defendant stating that his Private Information was involved in the Data Breach.

301. Plaintiff Berger is very careful about sharing his sensitive information.

302. Plaintiff Berger stores documents containing his Private Information in a safe and secure location.

303. Because of the Data Breach, Plaintiff Berger's Private Information is now in the hands of cybercriminals and on the dark web.

304. Plaintiff Berger has suffered actual injury from the exposure and theft of their Private Information—which violates his right to privacy.

305. As a result of the Data Breach, which exposed highly valuable Private Information, Plaintiff Berger is now imminently at risk of crippling future identity theft and fraud.

306. As a result of the Data Breach, Plaintiff Berger has been forced to spend at least five hours attempting to mitigate the harms caused and risks created by the Data Breach. Among other things, Plaintiff Berger has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account and provider statements and other information, and enrolling in credit monitoring services.

307. As a result of the Data Breach, Plaintiff Berger enrolled in Experian Credit Monitoring, which costs him $21.99 per month. Plaintiff Berger was not offered credit monitoring services by Defendant, and Plaintiff Berger's out-of-pocket losses for these services are an actual and ongoing injury caused by Defendant.

308. As a result of the Data Breach, Plaintiff Berger has experienced stress, anxiety, and concern because his private personal and medical information has been publicly exposed and is in the hands of cybercriminals.

309. Plaintiff Berger has already spent considerable time and money, and he anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

310. Plaintiff Berger has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of his valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Berger's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that

obligation by failing to provide reasonable and adequate data security to protect Plaintiff Berger's Private Information; and (e) continued risk to Plaintiff Berger's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF SARAH CROWELL'S EXPERIENCE

311. Plaintiff Sarah Crowell ("Plaintiff Crowell") entrusted her and her children's Private Information to Defendant as she and her family were near lifelong patients of Defendant.

312. Plaintiff Crowell's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

313. Plaintiff Crowell received a Data Breach notification letter from Defendant stating that her Private Information was involved in the Data Breach.

314. Plaintiff Crowell is very careful about sharing her and her children's sensitive information.

315. Plaintiff Crowell stores documents containing her and her children's Private Information in a safe and secure location.

316. Because of the Data Breach, Plaintiff Crowell's Private Information is now in the hands of cybercriminals and on the dark web.

317. Plaintiff Crowell has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

318. As a result of the Data Breach, which exposed highly valuable Private Information, Plaintiff Crowell and her children are now imminently at risk of crippling future identity theft and fraud.

319. As a result of the Data Breach, Plaintiff Crowell has been forced to spend several hours attempting to mitigate the harms caused and risks created by the Data Breach. Among other things, Plaintiff Crowell has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate the future consequences of the Data Breach, including researching facts about the Data Breach and thoroughly reviewing her and her children's statements and other information.

320. As a result of the Data Breach, Plaintiff Crowell has experienced stress, anxiety, and concern because her and her children's private information has been publicly exposed and is in the hands of cybercriminals.

321. Plaintiff Crowell has already spent considerable time, and she anticipates spending additional time on an ongoing basis to remedy the harms caused by the Data Breach.

322. Plaintiff Crowell has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of her valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Crowell's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Crowell's Private Information; and (e) continued risk to Plaintiff Crowell and her

children's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF ERIC WILSON'S EXPERIENCE

323. Plaintiff Eric Wilson ("Plaintiff Wilson") entrusted his Private Information to Defendant as a current patient of Defendant.

324. Plaintiff Wilson's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

325. Plaintiff Wilson received a Data Breach notification letter from Defendant stating that his Private Information was involved in the Data Breach.

326. Plaintiff Wilson is very careful about sharing his sensitive information.

327. Plaintiff Wilson stores any documents containing his Private Information in a safe and secure location.

328. Because of the Data Breach, Plaintiff Wilson's Private Information is now in the hands of cybercriminals and on the dark web.

329. Plaintiff Wilson has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

330. As a result of the Data Breach, which exposed his highly valuable Private Information, Plaintiff Wilson is now imminently at risk of crippling future identity theft and fraud.

331. As a result of the Data Breach, Plaintiff Wilson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Wilson has already expended

time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, signing up for credit monitoring and identity theft protection services, calling Defendant, thoroughly monitoring emails and financial statements, and taking other protective and ameliorative steps in response to the Data Breach.

332. As a result of the Data Breach, Plaintiff Wilson has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Wilson fears that criminals will use his information to commit identity theft.

333. Plaintiff Wilson has already spent considerable time, including the enrollment in credit monitoring protection, and anticipates spending additional time on an ongoing basis to remedy the harms caused by the Data Breach.

334. Plaintiff Wilson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Wilson's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Wilson's Private Information; and (e) continued risk to Plaintiff Wilson's Private Information, which remains in the possession of Defendant and which is subject to further breaches

so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF ERICA ORTIZ'S EXPERIENCE

335. Plaintiff Erica Ortiz ("Plaintiff Ortiz") entrusted her Private Information as a patient and employee of Defendant and the Private Information of her minor children as patients of Defendant.

336. Plaintiff Ortiz entrusted Defendant with her Private Information and the Private Information of her minor children with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

337. Plaintiff Ortiz received five Data Breach notification letters from Defendant stating that her Private information and that of each of her minor children was involved in the Data Breach.

338. Plaintiff Ortiz is very careful about sharing her sensitive information and that of her minor children.

339. Plaintiff Ortiz stores documents containing her Private Information or the Private Information of her minor children in a safe and secure location. Plaintiff Ortiz has never knowingly transmitted unencrypted sensitive Private Information of her minor children over the internet or any other unsecured source.

340. Because of the Data Breach, the Private Information of Plaintiff Ortiz and her minor children is now in the hands of cybercriminals and on the dark web.

341. Plaintiff Ortiz and her minor children have suffered actual injury from the exposure and theft of their Private Information—which violates their right to privacy.

342. Plaintiff Ortiz has also suffered actual injury because of obtaining and paying for data theft protection services which were necessitated by the Data Breach.

343. As a result of the Data Breach, which exposed highly valuable Private Information, Plaintiff Ortiz and each of her minor children are now imminently at risk of crippling future identity theft and fraud.

344. As a result of the Data Breach, Plaintiff Ortiz has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Ortiz has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her financial account statements for signs of fraud, monitoring phishing texts, signing up for data theft protection services, and attempting to sign up for data theft protection services for her minor children.

345. As a result of the Data Breach, Plaintiff Ortiz has experienced stress, anxiety, and concern due to the loss of her privacy and the privacy of her minor children. Plaintiff Ortiz is especially concerned as one of her minor children will soon be turning eighteen and is at substantial risk of identify theft. Plaintiff Ortiz fears that criminals will use the Private Information accessed in the Data Breach to commit identity theft.

346. Plaintiff Ortiz has already spent considerable time and money and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

347. Plaintiff Ortiz has also suffered injury directly and proximately caused by the Data Breach, including: (a) fraud; (b) theft of her and children's valuable Private Information; (c) the imminent and certainly impending injury flowing from fraud and identity theft posed by their Private Information being placed in the hands of cybercriminals; (d) damages to and/or diminution

in value of her and her children's Private Information that was entrusted to Defendant; (e) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff and her children should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff and her children's Private Information; and (f) continued risk to Plaintiff and her children's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF PATRICIA RODRIGUEZ'S EXPERIENCE

348. Plaintiff Patricia Rodriguez ("Plaintiff Rodriguez") entrusted her Private Information to Defendant as a patient of Defendant.

349. Plaintiff Rodriguez's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

350. Plaintiff Rodriguez received a Data Breach notification letter from Defendant stating that her Private Information was involved in the Data Breach.

351. Plaintiff Rodriguez is very careful about sharing her sensitive information.

352. Because of the Data Breach, Plaintiff Rodriguez's Private Information, including her Social Security number, is now in the hands of cybercriminals and on the dark web.

353. Plaintiff Rodriguez has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy. Plaintiff Rodriguez has additionally experienced an increase in spam calls, emails, and texts.

354. As a result of the Data Breach, which exposed her highly valuable Private Information, Plaintiff Rodriguez is now imminently at risk of crippling future identity theft and fraud.

355. As a result of the Data Breach, Plaintiff Rodriguez has had no choice but to spend several hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Rodriguez has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her account statements and Credit Karma reports, responding to and blocking spam calls, emails, and text messages, signing up for additional credit monitoring services, and taking other protective and ameliorative steps in response to the Data Breach.

356. As a result of the Data Breach, Rodriguez has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Rodriguez fears that criminals will use her information to commit identity theft. Further, Plaintiff Rodriguez was in the process of building her credit, and she is deeply anxious that the Data Breach will have a negative impact on her credit.

357. Plaintiff Rodriguez has already spent considerable time and anticipates spending additional time and possibly money on an ongoing basis to remedy the harms caused by the Data Breach.

358. Plaintiff Rodriguez has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Rodriguez's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution

in value of Plaintiff Rodriguez's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff Rodriguez, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Rodriguez's Private Information; and (e) continued risk to Plaintiff Pallman's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF ROBERT TAYLOR'S EXPERIENCE

359. Plaintiff Robert Taylor ("Plaintiff Taylor") entrusted his Private Information to Defendant as a patient of Defendant.

360. Plaintiff Taylor's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

361. Plaintiff Taylor received a Data Breach notification letter from Defendant stating that his Private Information was involved in the Data Breach.

362. Plaintiff Taylor is very careful about sharing his sensitive information.

363. Plaintiff Taylor stores any documents containing his Private Information in a safe and secure location.

364. Because of the Data Breach, Plaintiff Taylor's Private Information is now in the hands of cybercriminals and on the dark web.

365. Plaintiff Taylor has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy. Plaintiff Taylor discovered false credit

applications in his name in April 2025, which required him to contact the credit bureau. Plaintiff Taylor learned from one of his credit monitoring services which costs him $10 per month that his personal information was detected on the dark web in May 2025. Plaintiff Taylor has also suffered from an increase in spam calls and texts since March 2025, including someone calling to ask for his personal information in June 2025. Plaintiff Taylor further received an unusual email notifying him that a loan request could not be processed.

366. As a result of the Data Breach, which exposed his highly valuable Private Information and Social Security number, Plaintiff Taylor is now imminently at risk of crippling future identity theft and fraud.

367. As a result of the Data Breach, Plaintiff since April 2025 has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Hudson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and credit reports, responding to and blocking spam calls and text messages, dealing with suspicious account activity, and taking other protective and ameliorative steps in response to the Data Breach.

368. As a result of the Data Breach, Plaintiff Taylor has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Taylor fears that criminals will use his information to commit identity theft.

369. Plaintiff Taylor has already spent considerable time and money and anticipates spending additional time and money on an ongoing basis to remedy the harms caused by the Data Breach.

370. Plaintiff Taylor has also suffered injury directly and proximately caused by the Data Breach, including: (a) fraud; (b) theft of Plaintiff's valuable Private Information; (c) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Taylor's Private Information being placed in the hands of cybercriminals; (d) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant; (e) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Taylor's Private Information; and (f) continued risk to Plaintiff Taylor's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

PLAINTIFF TIFFANY ADJEI'S EXPERIENCE

371. Plaintiff Tiffany Adjei ("Plaintiff Adjei") entrusted her and her child's Private Information to Defendant.

372. Plaintiff Adjei's Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

373. Plaintiff Adjei received a Data Breach notification letter from Defendant stating that her Private Information was involved in the Data Breach.

374. Plaintiff Adjei is very careful about sharing her and her children's sensitive information.

375. Plaintiff Adjei stores documents containing her and her child's Private Information in a safe and secure location.

376. Because of the Data Breach, Plaintiff Adjei's Private Information is now in the hands of cybercriminals and on the dark web.

377. Plaintiff Adjei has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

378. As a result of the Data Breach, which exposed highly valuable Private Information, Plaintiff Adjei and her child are now imminently at risk of crippling future identity theft and fraud.

379. As a result of the Data Breach, Plaintiff Adjei has been forced to spend numerous hours attempting to mitigate the harms caused and risks created by the Data Breach. Among other things, Plaintiff Adjei has already expended time and suffered loss of productivity from taking time to address and attempt to mitigate the future consequences of the Data Breach, including researching facts about the Data Breach and thoroughly reviewing her and her child's statements and other information, responding to and blocking spam calls and text messages, changing sensitive information, and taking other protective and ameliorative steps in response to the Data Breach.

380. As a result of the Data Breach, Plaintiff Adjei has experienced stress, anxiety, and concern because her and her child's Private Information has been publicly exposed and is in the hands of cybercriminals.

381. Plaintiff Adjei has already spent considerable time, and she anticipates spending additional time on an ongoing basis to remedy the harms caused by the Data Breach.

382. Plaintiff Adjei has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of her valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Adjei's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Adjei's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff Adjei, including the difference in value between what Plaintiff Adjei should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Adjei's Private Information; and (e) continued risk to Plaintiff Adjei and her child's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

CLASS ALLEGATIONS

383. Plaintiffs bring this case individually and, pursuant to Federal Rule of Civil Procedure 23, on behalf of the following Class:

> **All individuals in the United States whose Private Information was compromised in the Defendant's Data Breach suffered on March 8, 2025**

384. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families. Plaintiffs reserve the right to modify or amend the definition of the proposed Class prior to moving for class certification.

385. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. It is believed the class size consists of over 5,600,000 Class Members. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

386. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had a duty to maintain the confidentiality of Plaintiffs' and Class Members' Private Information;

c. Whether Defendant breached its obligation to maintain Plaintiffs' and the Class Members' medical information in confidence;

d. Whether Defendant was negligent in collecting, storing and safeguarding Plaintiffs' and Class Members' Private Information, and breached its duties thereby;

e. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

f. Whether Plaintiffs and Class Members are entitled to restitution or disgorgement as a result of Defendant's wrongful conduct; and

g. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

387. **Typicality**. Plaintiffs' claims are typical of the claims of the Class Members. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard Private Information. Plaintiffs and Class Members were all patients or employees of Defendant, each having their Private Information stolen by an unauthorized third party.

388. **Adequacy of Representation.** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

389. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant breached its common law and statutory duties to secure Private Information on its network server, then Plaintiffs and each Class Member suffered damages from the exposure of sensitive Private Information in the Data Breach.

390. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

391. **Manageability.** The precise size of the Class is unknown without the disclosure of Defendant's records. The claims of Plaintiffs and the Class Members are substantially identical

as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiffs and the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

392. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

393. Defendant owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

394. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

395. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

396. Defendant breached the duties owed to Plaintiffs and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the

sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies to protect patients' Private Information.

397. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised and/or stolen.

398. Defendant also had a duty under Section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

399. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect the Private Information stolen in the Data Breach and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving the Private Information of its patients.

400. Plaintiffs and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

401. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

402. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act was intended to guard against.

403. Defendant violated its own policies not to use or disclose Private Information without written authorization.

404. Defendant violated its own policies by actively disclosing Plaintiffs' and the Class Members' Private Information; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information; and by failing to maintain the confidentiality of Plaintiffs' and the Class Members' records.

405. Defendant also had a duty under the Connecticut Data Privacy Act (CTDPA), which requires companies that process a certain amount of consumer personal data employ reasonable cybersecurity practices to prevent unauthorized access or theft. CGA § 42-515, *et seq.* All entities with operations in Connecticut that collect consumer health data are covered by CTDPA, including Defendant.

406. Defendant violated CTDPA by failing to employ reasonable cybersecurity practices to prevent unauthorized access or theft. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving the Private Information of its patients.

407. Plaintiffs and members of the Class are consumers within the class of persons CTDPA was intended to protect.

408. Defendant's violation of CTDPA constitutes negligence *per se*.

409. The harm that has occurred as a result of Defendant's conduct is the type of harm that CTDPA was intended to guard against.

410. Defendant also had a duty under HIPAA. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set

of security standards for protecting Private Information that is kept or transferred in electronic form.

411. Defendant violated HIPAA by failing to employ reasonable cybersecurity practices to prevent unauthorized access or theft. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving the Private Information of its patients.

412. Plaintiffs and members of the Class are consumers within the class of persons HIPAA was intended to protect.

413. Defendant's violation of HIPAA constitutes negligence *per se*.

414. The harm that has occurred as a result of Defendant's conduct is the type of harm HIPAA was intended to guard against.

415. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including: (a) actual misuse of their Private Information; (b) theft of their Private Information; (c) the substantial and imminent risk of identity theft; (d) invasion of privacy; (e) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (f) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (g) "out of pocket" costs incurred due to actual identity theft; (h) loss of time incurred due to actual identity theft and the substantial and imminent risk of identity theft; (i) loss of time due to increased spam and targeted marketing emails; (j) the loss of benefit of the bargain; (k) diminution in value of their Private Information; and (l) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

416. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

417. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

418. When Plaintiffs and members of the Class provided their Private Information to Defendant, Plaintiffs and members of the Class entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their data had been stolen in the Data Breach.

419. Defendant required Plaintiffs and Class Members to provide and entrust their Private Information as a condition of obtaining employment and/or services from Defendant.

420. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their Private Information to Defendant with the reasonable understanding that their Private Information would be adequately protected by Defendant from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive Private Information is exchanged as a condition of receiving medical services. It is common sense that but for this implicit and/or explicit agreement, Plaintiffs and Class Members would not have provided their Private Information to Defendant.

421. Defendant's contractual obligations are evidenced by its public facing privacy policy, which states that Defendant "understand[s] that medical information about you is personal. We are committed to protecting medical information about you."[54]

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

423. Plaintiffs and members of the Class fully performed their obligations under the implied contracts with Defendant.

424. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect the Private Information of Plaintiffs and members of the Class and by failing to provide timely notice to them that their Private Information was compromised and stolen in and as a result of the Data Breach.

425. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members have suffered (and will continue to suffer) concrete injuries, including: (a) actual misuse of their Private Information; (b) theft of their Private Information; (c) the substantial and imminent risk of identity theft; (d) invasion of privacy; (e) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (f) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (g) "out of pocket" costs incurred due to actual identity theft; (h) loss of time incurred due to actual identity theft and the substantial and imminent risk of identity theft; (i) loss of time due to increased spam and targeted marketing emails; (j) the loss of benefit of the bargain; (k) diminution in value of their Private Information; and (l) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches,

[54] *See* https://www.ynhhs.org/policies

so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

426. Thus, Plaintiffs 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.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

427. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

428. This count is brought in the alternative to Plaintiffs' breach of implied contract count. If claims for breach of contract are ultimately successful, this count will be dismissed.

429. Defendant benefited from receiving (a) payments made by or on behalf of Plaintiffs and Class Members for medical services they received, and (b) Plaintiffs' and Class Members' Private Information, by its ability to retain and use such payments and information for its own benefit, as part of Defendant's business and to gain profits. Defendant understood these benefits.

430. The valuable Private Information entrusted to Defendant, as well as the monies paid to Defendant by or on behalf of Plaintiffs and Class Members, were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiffs and Class Members.

431. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members, and as a result Defendant was overpaid.

432. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

433. Defendant was also enriched from the value of Plaintiffs' and Class Members' Private Information. Private Information has independent value as a form of intangible property. Defendant also derives value from this information because it allows Defendant to operate its business and generate revenue.

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

435. Under principles of equity and good conscience, Defendant should not be permitted to retain these benefits, including the money it intentionally refused to expend to safeguard the Private Information with which it had been entrusted, because Defendant failed to provide adequate safeguards and security measures to protect Plaintiffs' and Class Members' Private Information that they paid for but did not receive.

436. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class Members.

437. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

438. Plaintiffs and Class Members have no adequate remedy at law.

439. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered (and will continue to suffer) concrete injuries, including: (a) actual misuse of their Private Information; (b) theft of their Private Information; (c) the substantial and imminent risk of identity theft; (d) invasion of privacy; (e) "out of pocket" costs incurred mitigating the

materialized risk and imminent threat of identity theft; (f) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (g) "out of pocket" costs incurred due to actual identity theft; (h) loss of time incurred due to actual identity theft and the substantial and imminent risk of identity theft; (i) loss of time due to increased spam and targeted marketing emails; (j) the loss of benefit of the bargain; (k) diminution in value of their Private Information; and (l) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

440. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

FOURTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

441. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

442. In light of the special relationship between Defendant, as a medical provider, and Plaintiffs and Class Members, Defendant became a fiduciary by undertaking a guardianship of Plaintiffs' and Class Members' Private Information.

443. A physician has a fiduciary duty to not disclose a patient's medical information.

444. Defendant became a fiduciary, created by its undertaking and guardianship of Plaintiffs' and the Class Members' Private Information, to act primarily for the benefit of Plaintiffs and Class Members.

445. This duty included the obligation and responsibility to:

a. safeguard Plaintiffs' and Class Members' Private Information;

b. timely detect and notify Plaintiffs and the Class in the event of a data breach;

c. maintain adequate data security infrastructure, procedures, and protocols; and

d. establish and implement appropriate oversight and monitoring procedures for its employees.

446. In order to provide Plaintiffs and Class Members medical services, Defendant required that Plaintiffs and Class Members provide their Private Information to Defendant.

447. Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiffs' and Class Members' Private Information, for the benefit of Plaintiffs and Class Members and in order to provide Plaintiffs and Class Members with medical services.

448. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with them.

449. Defendant breached the fiduciary duties it owed to Plaintiffs and Class Members by failing to protect Plaintiffs' and Class Members' Private Information.

450. Defendant further breached the fiduciary duties it owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach and by failing to maintain adequate data security infrastructure, procedures, and protocols.

451. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer concrete injury, including, but not limited to: (i) actual misuse of their Private Information in the form of identity theft and fraud; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or

viewing of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, time and effort spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

452. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

453. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

454. This Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Consolidated Complaint.

455. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether Defendant is currently

maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs allege that Defendant's data security measures remain inadequate, contrary to Defendant's assertion that it has confirmed the security of its network. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of Private Information and remain at imminent risk that further compromises of Private Information will occur in the future.

456. Pursuant to its authority, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure Private Information and to timely notify employees, patients, or any individuals impacted by the Data Breach under the common law, Section 5 of the FTC Act, HIPAA, various state statutes, and the common law; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure current and former patients' Private Information.

457. This Court also should issue corresponding prospective injunctive relief requiring Defendant to, at minimum: (1) disclose, expeditiously, the full nature of the Data Breach, including when the Data Breach occurred, and the types of Private Information accessed, obtained, or exposed by the hackers; (2) implement improved data security practices to reasonably guard against future breaches of Plaintiffs' and Class Members' Private Information possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

458. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such

breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

459. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

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

461. Thus, the Court should issue prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect Plaintiffs' and Class Members' Private Information, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members; and

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

    i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and

ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. routinely and continually purging all former employee data that is no longer necessary in order to adequately conduct its business operations; meaningfully educating its current and former employees about the threats they face with regard to the security of their Private Information, as well as the steps Defendant's current and former employees should take to protect themselves.

462. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will

not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated, pray for relief as follows:

a. For an order certifying the Class under Federal Rule of Civil Procedure 23 and naming Plaintiffs as the representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

d. For an order of restitution, disgorgement, and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs' reasonable attorneys' fees, costs, and expenses;

g. Awarding pre and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: June 12, 2025

Respectfully Submitted,

/s/ Gary M. Klinger
Gary M. Klinger (admitted *Pro Hac Vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
gklinger@milberg.com

Mariya Weekes (admitted *Pro Hac Vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Tel: (786) 879-8200
Fax: (786) 879-7520
mweekes@milberg.com

Michael J. Reilly (CT# 28651)
CICCHIELLO & CICCHIELLO, LLP
364 Franklin Avenue
Hartford, CT 06114
Tel: 860-296-3457
Fax: 860-296-3457
mreilly@cicchielloesq.com

Jeff Ostrow (admitted *Pro Hac Vice*)
KOPELOWITZ OSTROW P.A.
1 West Las Olas Blvd., Ste. 500
Fort Lauderdale, FL 33301
Tel: (954) 332-4100
ostrow@kolawyers.com

Linda P. Nussbaum*
NUSSBAUM LAW GROUP P.C.
1133 Avenue of the Americas, 31st FL
New York, NY 10036
Tel: 917-438-9189
lnussbaum@nussbaumpc.com

Christian Levis*
Amanda G. Fiorilla*
Peter Demato*
Anthony M. Christina*
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
clevis@lowey.com
afiorilla@lowey.com
pdemato@lowey.com
achristina@lowey.com

Joseph P. Guglielmo (CT# 27481)
SCOTT+SCOTT
ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue
24th Floor
New York, NY 10169
Tel: (212) 223-6444
jguglielmo@scott-scott.com

Anja Rusi (CT# 30686)
SCOTT+SCOTT
ATTORNEYS AT LAW LLP
156 South Main Street
P.O. Box 192
Colchester, CT 06415
Tel.: (860) 537-5537
arusi@scott-scott.com

Michele S. Carino
GREENWICH LEGAL
ASSOCIATES LLC
Greenwich Legal Associates LLC
881 Lake Avenue
Greenwich, CT 06831
Tel: (203) 622-6001
mcarino@grwlegal.com

Kevin Laukaitis*
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
Tel: (215) 789-4462
klaukaitis@laukaitislaw.com

Gary F. Lynch*
Nicholas A. Colella*
Patrick D. Donathen*
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
gary@lcllp.com
nickc@lcllp.com
patrick@lcllp.com

William B. Federman (admitted *Pro Hac Vice*)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Tel: (405) 235-1560
wbf@federmanlaw.com

Oren Faircloth (CT# 438105)
Tyler J. Bean*
Neil P. Williams*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel: (212) 532-1091
ofaircloth@sirillp.com
tbean@sirillp.com
nwilliams@sirillp.com

Leanna A. Loginov*
SHAMIS GENTILE
14 NE 1st Ave., Suite 705
Miami, FL 33132
Tel: (305 479-2299
lloginov@shamisgentile.com

Joseph Kanee*
EDELSBERG LAW
20900 NE 30th Ave., Suite 417
Aventura, FL 33180
Tel: (786) 933-2775
Joseph@edelsberglaw.com

André Bélanger*
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Tel: (803) 222-2222
andre.belanger@poulinwilley.com

Jeremy C. Virgil (CT# 27707)
ZELDES, NEEDLE & COOPER, PC.
1000 Lafayette Blvd, 7th Floor
Bridgeport, CT 06604
Tel: (203) 333-9441
jvirgil@znclaw.com

Raina Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Tel: (872) 263-1100
raina@straussborrelli.com

Nicholas A. Migliaccio
Jason S. Rathod
MIGLIACCIO & RATHOD LLP
412 H St NE, Suite 302
Washington DC 20002
Tel: (202) 470-3520
jrathod@classlawdc.com

Samuel M. Ward*
BARRACK, RODOS & BACINE
One America Plaza
600 West Broadway, Suite 900
San Diego, CA 92101 sward@barrack.com
Tel.: (619) 230-0800
Facsimile: (619) 230-1874

Andrew Heo*
BARRACK, RODOS & BACINE
3300 Two Commerce Square
2001 Market Street
Philadelphia, PA 19103 aheo@barrack.com
Tel.: (215) 963-0600
Facsimile: (215) 963-0838

William M. Brown, Jr.
(D. Conn. # 20813)
William.brown@forthepeople.com
MORGAN & MORGAN, P.A.
199 Walter St., Suite 1500
New York, NY 10038
T: (917) 344-7039

JOHN A. YANCHUNIS*
jyanchunis@forthepeople.com
RONALD PODOLNY*
ronald.podolny@forthepeople.com
ANTONIO ARZOLA, JR.*
ararzola@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Phone: (813) 275-5272
Fax: (813) 222-4736

Mark S. Reich*
Melissa G. Meyer*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10006
Telephone: 212-363-7500
Facsimile: 212-363-7171
Email: mreich@zlk.com
mmeyer@zlk.com

(* denotes *pro hac vice* forthcoming)

Attorneys for the Plaintiffs and on Behalf of the Putative Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 12th day of June, 2025, a true copy of the foregoing was filed electronically using the Court's CM/ECF system, to be served via operation of the Court's electronic filing system upon all counsel of record.

/s/ Gary M. Klinger
Gary M. Klinger (admitted *Pro Hac Vice*)