IN THE SUPERIOR COURT FOR THE STATE OF WASHINGTON
IN AND FOR WHATCOM COUNTY

| | |
|---|---|
| GENEVIEVE BARDWELL, JEFF EBERLEIN, THOMAS SCHUMANN, JEFFREY KAHN, DANIEL UITDENHOWEN, MICHAEL BARR, LESLIE SWOPE, JOANNE HERMAN and NAOMI LIEBHOLD, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>MT. BAKER IMAGING, LLC and NORTHWEST RADIOLOGISTS, INC., P.S.,<br><br>Defendant. | NO. 25-2-00463-37<br><br>CONSOLIDATED CLASS ACTION COMPLAINT<br><br>DEMAND FOR A JURY TRIAL |

Plaintiffs Genevieve Bardwell, Jeff Eberlein, Thomas Schumann, Jeffrey Kahn, Daniel Uitdenhowen, Michael Barr, Leslie Swope, Joanne Herman and Naomi Liebhold ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Mt. Baker Imaging, LLC and Northwest Radiologists, Inc., P.S. (collectively, "Northwest/MBI" or "Defendants") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

## SUMMARY OF ACTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard the sensitive information of their patients.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

2. Defendant Mt. Baker is a Washington-based healthcare imaging provider that provides "precision imaging tools to local [healthcare] providers."[1] According to its website, Defendant Mt. Baker uses radiologists from Defendant Northwest Radiologists to interpret the images they collect. As part of their practice, Defendants collected and maintained certain personally identifiable information and protected health information of Plaintiffs and the putative Class Members.

3. In January 2025, Defendants learned that their computer systems had been compromised (the "Data Breach"). Together with a cybersecurity forensics firm, Defendants determined that "certain data was accessed by an unauthorized party." This data included protected health information, and specifically, "individuals' first and last names in combination with address information, telephone number, date of birth, email address, Social Security number, driver's license or state identification card number, treatment or diagnosis information, provider name, medical record number or patient identification number, health insurance information, and/or treatment cost information" (collectively "Private Information").[2]

4. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendants on the mutual understanding that Defendants would protect it against disclosure—was targeted, compromised and unlawfully accessed due to the Data Breach.

5. As a result of the Data Breach, Plaintiffs and Class Members suffered concrete injuries in fact including, but not limited to: (1) invasion of privacy; (2) theft of their Private Information; (3) lost or diminished value of Private Information; (4) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (5) loss of benefit of the bargain; (6) actual misuse of their Private Information consisting of an

[1] *See* https://mtbakerimaging.com/about-us-2/.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

increase in spam calls, texts, and/or emails; (7) nominal damages; and (8) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

6. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patients' Private Information from a foreseeable and preventable cyber-attack.

7. Moreover, upon information and belief, Defendants were targeted for a cyber-attack due to their status as a healthcare entity that collects and maintains highly valuable Private Information on their systems.

8. Defendants maintained, used, and shared the Private Information in a reckless manner. In particular, the Private Information was used and stored by Defendants in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack—and potential for improper disclosure of Plaintiffs' and Class Members' Private Information—was a known risk to Defendants, and thus, Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

9. Defendants disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide

[2] https://mtbakerimaging.com/notification/.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

10. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct because the Private Information that Defendants collected and maintained has been accessed and acquired by data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, giving false information to police during an arrest, receiving health care services in Class Members' names using their insurance, and committing health care insurance fraud.

12. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiffs and Class Members may also incur out-of-pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. Plaintiffs bring this class action lawsuit on behalf of all those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

15. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

16. Plaintiffs and Class Members have a continuing interest in ensuring their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

## JURISDICTION AND VENUE

17. The Court has original jurisdiction over this action under RCW 2.08.010.

18. This Court has personal jurisdiction over Defendants because Defendants are incorporated and headquartered in Washington State and this county.

19. Venue is proper in this county under RCW 4.12.025 because a substantial part of the events or omissions giving rise to Plaintiffs' and Class Members' claims occurred in this county and because Defendants' principal place of business is in this county.

## PARTIES

20. Plaintiff Bardwell is a resident and citizen of Washington.

21. Plaintiff Schumann is a resident and citizen of Washington.

22. Plaintiff Kahn is a resident and citizen of Washington.

23. Plaintiff Eberlein is a resident and citizen of Washington.

24. Plaintiff Uitdenhowen is a resident and citizen of Washington.

25. Plaintiff Barr is a resident and citizen of Washington.

26. Plaintiff Swope is a resident and citizen of Washington.

27. Plaintiff Herman is a resident and citizen of Washington.

28. Plaintiff Liebhold is a resident and citizen of Washington.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

29. Defendant Mt. Baker Imaging, LLC is a limited liability company organized under the laws of the state of Washington with its principal place of business located in Bellingham, Washington.

30. Defendant Northwest Radiologists, Inc., P.S., is a professional services corporation organized under the laws of the state of Washington with its principal place of business located in Bellingham, Washington.

## FACTUAL ALLEGATIONS

***Defendants' Business***

31. Defendants are Washington-based healthcare imaging providers that provide imaging and interpretive services to patients and other healthcare organizations.

32. Plaintiffs and Class Members are current and former patients of Defendants.

33. In the course of their relationship, patients, including Plaintiffs and Class Members, provided Defendants with at least the following: names, dates of birth, Social Security numbers, healthcare treatment information, and other sensitive information.

34. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiffs, Defendants promised to provide confidentiality and adequate security for the data they collected from patients through their applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

35. Plaintiffs and the Class Members, as patients at Defendants, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Private Information, especially when their Social Security numbers, health care information, and other sensitive Private Information is involved.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

***The Data Breach***

36. On or about March 26, 2025, Defendants posted a Notification of Data Security Incident on their website (the "Website Notice"), informing them that:

> On or around January 25, 2025, Northwest Radiologists and Mount Baker Imaging ("Northwest/MBI"), experienced a network disruption that impacted certain systems and immediately began investigating with the assistance of third-party computer forensic specialists. The investigation determined that certain data was accessed by an unauthorized party. Therefore, we are currently reviewing the types of information potentially impacted by this event; however, Northwest/MBI has confirmed that a limited amount of protected health information may have been impacted in connection with this event.
>
> Although the review is ongoing, the types of information generally might have included individuals' first and last names in combination with address information, telephone number, date of birth, email address, Social Security number, driver's license or state identification card number, treatment or diagnosis information, provider name, medical record number or patient identification number, health insurance information, and/or treatment cost information. Northwest/MBI has established a dedicated call center to answer questions about the event and to address related concerns.[3]

37. To date, Defendants have not provided individual notice to Class Members.

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

39. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts.

[3] https://mtbakerimaging.com/notification/.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

40. Despite Defendants' intentional opacity about the root cause of this incident, several facts may be gleaned from the Website Notice, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendants' networks and systems and accessed data; and c) that once inside Defendants' networks and systems, the cybercriminals targeted information including Plaintiffs' and Class Members' Private Information.

41. In the context of data breach Website Notices of this type, Defendants' use of the phrase "might have included" is misleading legal language. Companies only issue Website Notices because data breach notification laws require them to do so. Such notices are made only where Defendants have a reasonable belief that their personal information was accessed or acquired by an unauthorized individual or entity. Defendants cannot hide behind legalese—by issuing a notice of data breach, Defendants implicitly admit that they had a reasonable belief that unknown actors, aka cybercriminals, accessed or acquired Plaintiffs' and Class Members' names, Social Security numbers, PHI, and other sensitive information.

42. Moreover, in their Website Notice, Defendants failed to (a) specify whether they undertook any efforts to find out if Class Members whose data was accessed and acquired in the Data Breach had suffered misuse of their data; (b) indicate that Defendants were interested in hearing about misuse of their data; or (c) set up a mechanism for Class Members to report misuse of their data.

43. Defendants had obligations created by the FTC Act, HIPAA, contract, common



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

44. Because Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, such as encrypting the information or deleting it when it is no longer needed, Defendants allowed the exposure of Private Information.

45. The attacker accessed files containing Plaintiffs' and Class Members' unencrypted Private Information.

***Data Breaches Are Preventable***

46. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, such as encrypting the information or deleting it when it is no longer needed, thereby causing the exposure of Private Information,

47. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

48. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[4]

49. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented the following measures recommended by the United States Government:

[4] How to Protect Your Networks from RANSOMWARE at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

- Implement an awareness and training program to ensure targeted end users are aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices, optimally with a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[5]

[5] *Id.* at 3–4.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

50. To prevent and detect cyber-attacks or ransomware attacks, Defendants could and should have implemented the following measures recommended by the Microsoft Threat Protection Intelligence Team:

**Secure Internet-Facing Assets**

- Apply latest security updates;
- Use threat and vulnerability management; and
- Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

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

**Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins by configuring servers and other endpoints securely;

**Build credential hygiene**

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

**Apply principle of least-privilege**

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs; and
- Analyze logon events;

**Harden infrastructure**

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection; and
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[6]

[6] *See Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

51. Given that Defendants were storing the Private Information of their current and former patients, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

52. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves accessing the Private Information of Plaintiffs and Class Members.

***Defendants Acquire, Collect, and Store Patients' Private Information***

53. Defendants acquire, collect, and store a massive amount of Private Information of their current and former patients.

54. As a condition of becoming a patient of Defendants, Defendants require that patients entrust them with highly sensitive personal information.

55. By obtaining, collecting, and using Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

56. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendants absent a promise to safeguard that information.

57. Upon information and belief, Defendants promised in privacy policies and other legally required disclosures to treat the Private Information they collected from patients, including that of Plaintiffs, as confidential and to provide adequate security for it.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

58. Plaintiffs and the Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

***Defendants Knew, or Should Have Known, of the Risk Because Healthcare Entities in Possession of Private Information Are Particularly Susceptible to Cyber Attacks***

59. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendants, preceding the date of the breach.

60. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

61. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[7]

62. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

63. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

[7] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

64. Additionally, as companies became more dependent on computer systems to run their business,[9] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[10]

65. Defendants knew and understood unprotected or exposed Private Information in the custody of healthcare entities, like Defendants, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

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

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

---

[8] https://www.law360.com/patientprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=patientprotection.

[9]https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

68. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

69. The ramifications of Defendants' failure to secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

70. As healthcare entities in custody of the Private Information of patients, Defendants knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiffs and Class Members, and of the foreseeable consequences if those data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

***Value of Private Information***

71. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number,

[10] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.

[11] 17 C.F.R. § 248.201 (2013).



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

government passport number, employer or taxpayer identification number."[12]

72. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials.[13]

73. For example, Private Information can be sold at a price ranging from $40 to $200.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

74. Moreover, Social Security numbers, which were compromised for some Class Members in the Data Breach, 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.

75. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [16] Moreover, "[b]ecause many organizations still use SSNs as the

---

[12] *Id.*

[13] *Your personal data is for sale on the Dark Web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[15] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[16] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

primary identifier, exposure to identity theft and fraud remains."[17]

76. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

77. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[19] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[20]

78. 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.

79. Even then, a new Social Security number may not be effective. According to

---

[17] *Id.*

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

[19] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/.

[20] *See* https://www.investopedia.com/terms/s/ssn.asp.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Julie Ferguson of the Identity Theft Resource Center, "[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."[21]

80. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), *report and recommendation adopted*, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiffs' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, . . . tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.").

81. Similarly, the California state government warns patients that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the

[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[22]

82. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[23]

83. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the Dark Web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post on several underground internet websites stolen payment card numbers, Social Security numbers, and other personal information. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

84. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[24] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[25] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of

---

[22] *See* https://oag.ca.gov/idtheft/facts/your-ssn.

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

[24] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/.

[25] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

overall health data breaches, according to cybersecurity firm Tenable.[26]

85. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[27]

86. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[28]

87. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[29] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[30]

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

[26] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/.

[27] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

[28] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

[29] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

the black market."[31]

89. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, PHI, dates of birth, and names.

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

91. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[32]

92. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will

---

[30] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/.

[31] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at* https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html .



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

continue to incur such damages in addition to any fraudulent use of their Private Information.

***Defendants Failed to Comply with FTC Guidelines***

93. 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.

94. 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 patient 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.[33]

95. 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.[34]

96. 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

---

[32] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf.

[33] *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 .

[34] *Id.*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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

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

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

99. 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 Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

100. Defendants failed to properly implement basic data security practices.

101. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information of their patients 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.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

102. Upon information and belief, Defendants were at all times fully aware of their obligation to protect the Private Information of patients. Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

***Defendants Failed to Comply with HIPAA Guidelines***

103. Defendants are covered entities under HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

104. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[35] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

105. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

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

107. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

information." 45 C.F.R. § 164.302.

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

109. HIPAA's Security Rule requires Defendants to do the following:

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

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

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

d. Ensure compliance by their workforce.

110. HIPAA also requires Defendants 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, Defendants are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

111. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against

[35] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

112. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[36]

113. HIPAA requires a covered entity to have and apply appropriate sanctions against personnel 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).

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

115. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis

[36] *Breach Notification Rule*, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).



**TOUSLEY BRAIN STEPHENS PLLC**
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

requirements of the Security Rule."[37] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."[38]

116. Defendants' Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

***Defendants Failed to Comply with Industry Standards***

117. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

118. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendants. Those practices include, but are not limited to, educating all employees; employing strong passwords; implementing multi-layer security, including firewalls, anti-virus, and anti-malware software; encrypting data to make it unreadable without a key; requiring multi-factor authentication; backing up data and limiting which employees can access sensitive data. Defendants failed to follow all of these industry best practices.

119. Other best cybersecurity practices that are standard for healthcare entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protecting physical security systems; safeguarding all possible communication systems; and training staff regarding critical points.

[37] HHS, *Security Rule Guidance Material*, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Defendants failed to follow all these cybersecurity best practices, including failure to train staff.

120. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

121. These foregoing frameworks are existing and applicable industry standards for healthcare entities, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

***Common Injuries & Damages***

122. As a result of Defendants' ineffective and inadequate data security practices, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further

[38] HHS, *Guidance on Risk Analysis*, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

***Data Breaches Increase Victims' Risk of Identity Theft***

123. The unencrypted Private Information of Class Members will very likely end up for sale on the Dark Web, as that is the modus operandi of hackers.

124. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

125. 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.

126. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

127. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes."[39]

128. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier. . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective patients."[40]

129. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest twenty-five banks have stopped using the numbers to verify a patient's identity after the initial account setup."[41] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"[42]

130. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[43]

---

[39] *See* N.C. Gen. Stat. § 132-1.10(1).

[40] *See* https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers.

[41] *See* https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/.

[42] *See* https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[43] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the Dark Web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

131. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

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

133. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiffs and the other Class Members.

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

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

***Loss of Time to Mitigate Risk of Identity Theft & Fraud***

136. 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 compromised, as

---

*Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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 and 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.

137. The steps that Plaintiffs and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant time that Plaintiffs and Class Members must undertake in response to the Data Breach. Plaintiffs' and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiffs and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach.

138. Plaintiffs and Class Members have spent, and will spend additional time, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, signing up for the credit monitoring services, and monitoring their financial accounts for any unusual activity, which may take years to detect. Accordingly, the Data Breach has caused Plaintiffs and Class Members to suffer actual injury in the form of lost time spent on mitigation activities—which cannot be recaptured.

139. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that 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

---

stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

damage to their good name and credit record."[44]

140. Plaintiffs' mitigation efforts are also consistent with the steps the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[45]

***Diminution of Value of Private Information***

141. PII and PHI are valuable property.[46] Their value is axiomatic, 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.

142. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[47]

143. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[48]

---

[44] *See* United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[45] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

[46] *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").

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



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

144. In fact, the data marketplace is so sophisticated that patients 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.[49,50]

145. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[51]

146. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[52]

147. 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 by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

148. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the

---

cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[48] *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/.

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

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

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

[52] *See Medical I.D. Theft*, *supra* note 23.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

149. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

151. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting on information and belief to more thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

152. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

***Loss of Benefit of The Bargain***

153. Furthermore, Defendants' poor data security practices deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendants and/or their agents for medical products and/or services, Plaintiffs and other reasonable patients understood and expected that they were, in part, paying for the services and necessary data security to protect their Private Information, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiffs and Class Members received products and/or services that



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

**REPRESENTATIVE PLAINTIFFS' EXPERIENCES**

***Plaintiff Genevieve Bardwell's Experience***

154. Plaintiff Genevieve Bardwell is and at times mentioned herein was a patient of Defendant Mt. Baker since approximately October 2024.

As a condition of receiving healthcare services, Plaintiff was required to provide her sensitive personal and medical information to Defendants.

Plaintiff provided her Sensitive Information to Defendants with the reasonable expectation that Defendants would protect and secure this information from unauthorized access and disclosure.

On information and belief, Plaintiff's Sensitive Information, including her name, date of birth, address, Social Security number, driver's license number, medical record number, lab results, treatment information, health insurance information, provider names, and/or financial information, was improperly accessed or obtained by unauthorized third parties when the Data Breach occurred.

Plaintiff reasonably expected and understood that Defendants would take, at a minimum, industry standard precautions to protect, maintain, and safeguard her Sensitive Information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to the same. Plaintiff would not have used Defendants' services had she known that Defendants would not take reasonable steps to safeguard her Sensitive Information.

Plaintiff is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

source. Furthermore, Plaintiff stores any documents containing her sensitive information in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial statements, monitoring her credit information, and changing passwords on her various accounts.

Upon information and belief, Plaintiff Bardwell suffered actual injury from having her sensitive information exposed and/or stolen as a result of the Data Breach.

***Plaintiff Jeff Eberlein's Experience***

Plaintiff Jeff Eberlein has received medical services from Defendants.

On or about April 9, 2025, Plaintiff learned of the Data Breach, and became informed of the substantive details of the Data Breach based on Defendants' Notification of Data Security Incident which is posted on their website.[53]

Following the Data Breach, Plaintiff has experienced a substantial uptick in the number and frequency of spam emails, as well as a significant increase in spam phone calls – something that was not a frequent occurrence prior to the date of the Data Breach.

Plaintiff has made, and will continue to make, reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach; reviewing credit reports, medical records, credit monitoring, and financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Defendants; and dealing with unwanted spam emails, texts, and

[53] *Id.*



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

telephone calls.

Since Plaintiff became aware of the Data Breach, he has already spent hours dealing with the Data Breach, which is valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

As a result of the Data Breach, Plaintiff has suffered emotional distress due to the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his Private Information, a form of property that Defendants obtained from Plaintiff; (b) violation of his privacy rights; (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud, and (d) identity theft as defined by RCW 9.35.020(1).

As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

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

***Plaintiff Jeffrey Kahn's Experience***

155. Plaintiff Jeffrey Kahn has received medical services from Defendants.

156. As a condition of obtaining services from Defendants, he was required to provide his Private Information to Defendants, including his name, date of birth, Social



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Security number, and other sensitive information, including health information.

157. Upon information and belief, at the time of the Data Breach, Defendants maintained Plaintiff's Private Information in their systems.

158. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

159. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

160. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

//

//



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

***Plaintiff Leslie Swope's Experience***

162. Plaintiff Swope has received medical services from Defendants and provided her Private Information to Defendants in exchange for services.

163. At the time of the Data Breach, Defendants retained Plaintiff's Private Information in their system.

164. Plaintiff's Private Information was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendants' network for the specific purpose of targeting the Private Information.

165. Plaintiff takes reasonable measures to protect her Private Information. She has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

166. Plaintiff stores any documents containing her Private Information in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

167. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend time monitoring her account and credit score and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

168. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that she entrusted to Defendants for the purpose of obtaining services from Defendants, which was compromised in and as a result of the Data Breach.

169. Since the Data Breach, Plaintiff has experienced an increase in spam calls and



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

texts.

170. Plaintiff suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

171. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, especially her name, Social Security number, and PHI, being placed in the hands of criminals.

172. Defendants obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of the Data Breach.

173. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

***Plaintiff Joanne Herman's Experience***

174. Plaintiff Herman has received medical services from Defendants and provided her Private Information to Defendants in exchange for services.

175. At the time of the Data Breach, Defendants retained Plaintiff's Private Information in their system.

176. Plaintiff's Private Information was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendants' network for the specific purpose of targeting the Private Information.



**TOUSLEY BRAIN STEPHENS PLLC**
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

177. Plaintiff takes reasonable measures to protect her Private Information. She has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

178. Plaintiff stores any documents containing her Private Information in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

179. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend time monitoring her account and credit score and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

180. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that she entrusted to Defendants for the purpose of obtaining services from Defendants, which was compromised in and as a result of the Data Breach.

181. Since the Data Breach, Plaintiff has experienced an increase in spam calls and texts.

182. Plaintiff suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

183. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, especially her name, Social Security number, and PHI, being placed in the hands of criminals.

184. Defendants obtained and continues to maintain Plaintiff's Private Information



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of the Data Breach.

185. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

***Plaintiff Naomi Liebhold Experience***

186. Plaintiff Liebhold has received medical services from Defendants and provided her Private Information to Defendants in exchange for services.

187. At the time of the Data Breach, Defendants retained Plaintiff's Private Information in their system.

188. Plaintiff's Private Information was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendants' network for the specific purpose of targeting the Private Information.

189. Plaintiff takes reasonable measures to protect her Private Information. She has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

190. Plaintiff stores any documents containing her Private Information in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

191. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend time monitoring her account and credit score and has sustained



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

192. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that she entrusted to Defendants for the purpose of obtaining services from Defendants, which was compromised in and as a result of the Data Breach.

193. Since the Data Breach, Plaintiff has experienced an increase in spam calls and texts.

194. Plaintiff suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

195. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, especially her name, Social Security number, and PHI, being placed in the hands of criminals.

196. Defendants obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of the Data Breach.

197. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

198. As a result of the Data Breach, Plaintiff is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

***Plaintiff Daniel Uitdenhowen's Experience***

199. Plaintiff Daniel Uitdenhowen has received medical services from Defendants.

200. As a condition of obtaining medical services from Defendants, he was required to provide his Private Information to Defendants, including his name, date of birth, Social Security number, and other sensitive information, including health information.

201. Upon information and belief, at the time of the Data Breach, Defendants maintained Plaintiff's Private Information in their systems.

202. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to formally and promptly notify him.

203. As a result of their inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

204. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

205. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

206. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

207. Plaintiff has suffered actual injury in the form of damages to and diminution in



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

the value of his Sensitive Information---a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

208. Plaintiff suffered actual injury from the exposure of his Sensitive Information---which violates his rights to privacy.

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

210. Indeed, following Data Breach, Plaintiff began receiving emailed receipts for purchases that he did not recognize and certainly did not authorize. As a result, Plaintiff has been forced to spend significant amounts of time and effort verifying the legitimacy of these emailed receipts. Furthermore, these emails suggest that his Sensitive Information is now in the hands of cybercriminals.

211. Plaintiff is also experiencing a significant increase in spam texts and phone calls following the breach, further suggesting that his Sensitive Information is now in the hands of cybercriminals.

212. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

213. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

214. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

***Plaintiff Michael Barr's Experience***

216. Plaintiff Michael Barr has received medical services from Defendants.

217. As a condition of obtaining medical services from Defendants, he was required to provide his Private Information to Defendants, including his name, date of birth, Social Security number, and other sensitive information, including health information.

218. Upon information and belief, at the time of the Data Breach, Defendants maintained Plaintiff's Private Information in their systems.

219. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to formally and promptly notify him.

220. As a result of their inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

221. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

be recaptured.

222. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

223. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

224. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of his Sensitive Information---a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

225. Plaintiff suffered actual injury from the exposure of his Sensitive Information---which violates his rights to privacy.

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

227. Indeed, following Data Breach, Plaintiff is now experiencing a significant increase in spam texts, suggesting that his Sensitive Information is now in the hands of cybercriminals.

228. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

229. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

230. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

***Plaintiff Thomas Schumann's Experience***

232. Plaintiff Thomas Schumann has received medical services from Defendants.

233. As a condition of obtaining medical services from Defendants, he was required to provide his Private Information to Defendants, including his name, date of birth, Social Security number, and other sensitive information, including health information.

234. Upon information and belief, at the time of the Data Breach, Defendants maintained Plaintiff's Private Information in their systems.

235. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

236. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

237. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

## CLASS ALLEGATIONS

239. Pursuant to Washington Civil Rule 23, Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported by Defendants in March 2025 (the "Class").

240. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

241. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

242. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendants, upon information and belief, thousands of individuals were impacted.

243. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Included among the questions of law and fact common to the Class that predominate over questions which may affect individual Class Members, are the following:

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

b. Whether Defendants had a duty to not disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had the duty to not use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages, treble damages, and/or nominal damages as a result of Defendants' wrongful conduct;

k. 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.

244. Typicality: Plaintiffs' claims are typical of those of the other patients of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as every other member of the Class.

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



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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

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

248. The nature of this action and the nature of laws available to Plaintiffs and Class Members makes the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

250. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

## COUNT I
## Negligence
## (On Behalf of Plaintiffs and the Class)

251. Plaintiffs reallege and incorporate by reference all of the above paragraphs, as if fully set forth herein.

252. Defendants require their patients, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing their healthcare services.

253. Defendants gathered and stored the Private Information of Plaintiffs and Class Members as part of their business of soliciting their services to patients.

254. Plaintiffs and Class Members entrusted Defendants with their Private Information with the understanding that Defendants would safeguard their information.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

255. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed.

256. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

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

259. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

260. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their patients. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential Private Information, a necessary part of being patients of Defendants.

261. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

262. Defendants are subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

263. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information they were no longer required to retain pursuant to regulations.

264. Moreover, Defendants had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

265. Defendants had and continue to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

266. Defendants breached their duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information.

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

268. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

269. Defendants' violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

270. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

271. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

272. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

273. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

274. Plaintiffs and the Class were the foreseeable and probable victims of any



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems.

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

276. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

277. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

278. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

279. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (1) invasion of privacy; (2) theft of their Private Information; (3) lost or diminished value of Private Information; (4) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (5) loss of benefit of the bargain; (6) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (7) nominal damages; and (8) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

280. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

281. Defendants' negligent conduct is ongoing, since they still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

282. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**COUNT II**
**Breach of Implied Contract**
**(On Behalf of Plaintiffs and the Class)**

283. Plaintiffs reallege and incorporate by reference all of the above paragraphs, as if fully set forth herein.

284. Plaintiffs and Class Members were required to provide their Private Information to Defendants as a condition of receiving healthcare services from Defendants.

285. Plaintiffs and the Class entrusted their Private Information to Defendants. In so doing, Plaintiffs and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

286. Implicit in the agreement between Plaintiffs and Class Members and the Defendants to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

287. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendants, on the other, is demonstrated by their conduct and course of dealing.

288. Defendants solicited, offered, and invited Plaintiffs and Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

289. In accepting the Private Information of Plaintiffs and Class Members, Defendants understood and agreed that they were required to reasonably safeguard the Private Information from unauthorized access or disclosure.

290. On information and belief, at all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby they expressly promised Plaintiffs and Class Members that they would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

291. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

292. In entering into such implied contracts, Plaintiffs and Class Members reasonably



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

293. Plaintiffs and Class Members paid money to Defendants with the reasonable belief and expectation that Defendants would use part of their earnings to obtain adequate data security. Defendants failed to do so.

294. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

295. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

296. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

297. Defendants breached the implied contracts they made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

298. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

299. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

300. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT III**
**Invasion of Privacy—Intrusion Upon Seclusion**
**(On Behalf of Plaintiffs and the Class)**

301. Plaintiffs reallege all previous paragraphs as if fully set forth below.

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

303. Defendants owed a duty to their patients, including Plaintiffs and the Class, to keep this information confidential.

304. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Sensitive Information is highly offensive to a reasonable person.

305. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendants as part of their receipt of medical services from Defendants, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

307. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

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

309. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

310. As a proximate result of Defendants' acts and omissions, the Sensitive Information of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

311. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class because their Sensitive Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

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

313. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other members of the Class, also seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

**COUNT IV**
**Violation of the Washington Consumer Protection Act**
**RCWA §§ 19.86.010, *et seq.*,**
**(On Behalf of Plaintiffs and the Class)**

314. Plaintiffs reallege and incorporate by reference all of the above paragraphs, as if fully set forth herein.

315. Defendants are each a "person," as defined by RCW 19.86.010(1).

316. Defendants advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by RCW 19.86.010 (2).

317. Defendants engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of RCW 19.86.020, including:

a. By failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Private Information, which was a direct and proximate cause of the data breach;

a. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act and HIPAA;



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

c. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

d. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' PII, including duties imposed by the FTC Act and HIPAA;

e. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; and

f. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act and HIPAA.

318. Defendants' representations and omissions were material because they were likely to deceive reasonable employees about the adequacy of Defendants' data security and ability to protect the confidentiality of patients' Private Information.

319. Defendants acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Class Members' rights. Numerous past data breaches put them on notice that their security and privacy protections were inadequate.

320. Defendants' conduct is injurious to the public interest because it violates RCW 19.86.020, a statute that contains a specific legislative declaration of public interest impact, and/or they injured persons and has the capacity to injure persons. Further, their conduct affected the public interest, including the thousands of Washingtonians affected by the data breach.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

321. As a direct and proximate result of Defendants' unfair or deceptive acts or practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and their Private Information's loss of value.

322. Plaintiffs and Class Members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

**COUNT V**
**Violation of the Washington Data Breach Notification Disclosure Law**
**RCW 19.255.005 *et seq*.**
**(On Behalf of Plaintiffs and the Class)**

323. Plaintiffs reallege and incorporate by reference all of the above paragraphs, as if fully set forth below.

324. Under RCW 19.255.010(2), "[a]ny person or business that maintains or possesses data that may include personal information that the person or business does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery[.]"

325. On information and belief, this statute applies to Defendant because Defendant does not own nor license the Sensitive Information exposed.

326. The Data Breach at issue constitutes a "breach of the security of the data" under RCW 19.255.010.

327. Defendants violated the Washington Data Breach Notification Disclosure Law when they failed to disclose the Data Breach to Plaintiffs and Class Members "immediately



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

following discovery" nor in a reasonable timely manner. Thus, Plaintiffs seek all available relief.

**COUNT VI**
**Violation of the Uniform Health Care Information Act**
**RCW 70.02.005 *et seq*.**
**(On Behalf of Plaintiffs and the Class)**

328. Plaintiffs reallege all previous paragraphs as if fully set forth below.

329. The Uniform Health Care Information Act (UHCIA) declares that:

330. "Health care information is personal and sensitive information that if improperly used or released may do significant harm to a patient's interests in privacy, health care, or other interests." § 70.02.005(1).

331. "In order to retain the full trust and confidence of patients, health care providers have an interest in assuring that health care information is not improperly disclosed and in having clear and certain rules for the disclosure of health care information." § 70.02.005(3).

332. "It is the public policy of this state that a patient's interest in the proper use and disclosure of the patient's health care information survives even when the information is held by persons other than health care providers." § 70.02.005(4).

333. Here, Defendants are a "health care provider" because Defendants are "licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession." § 70.02.010(19).

334. Under § 70.02.020, "a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization."



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

335. Here, Defendants violated UHCIA because Defendant—via the Data Breach—disclosed health care information to third parties without patient authorization. Thus, Plaintiffs seeks injunctive relief, equitable relief, and actual damages.

**COUNT VII**
**Violation of the Washington My Health My Data Act**
**RCW 19.373 *et seq*.**
**(On Behalf of Plaintiffs and the Class)**

336. Plaintiffs reallege all previous paragraphs as if fully set forth below.

337. RCW 19.373.005 provides that "the legislature intends to provide heightened protections for Washingtonian's health data[.]"

338. RCW 19.373.030 provides that "beginning March 31, 2024" a "regulated entity or a small business may not share any consumer health data[.]"

339. RCW 19.373.050 provides that "beginning March 31, 2024, a regulated entity and a small business shall: (a) Restrict access to consumer health data by the employees, processors, and contractors of such regulated entity or small business to only those employees, processors, and contractors for which access is necessary to further the purposes for which the consumer provided consent or where necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business; and (b) Establish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy reasonable standard of care within the regulated entity's or the small business's industry to protect the confidentiality, integrity, and accessibility of consumer health data appropriate to the volume and nature of the consumer health data at issue."

340. Furthermore, under 19.373.090, a violation of this Act "is not reasonable in relation to the development and preservation of business, and is an unfair or deceptive act in



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW."

341. Here, Defendants' failure to secure Plaintiffs' and Class Members' Sensitive Information—which resulted in the Data Breach—constitute violations of the Washington My Health My Data Act. Thus, Plaintiffs seek all available relief.

**COUNT VIII**
**Unjust Enrichment**
**(On Behalf of Plaintiffs and the Class)**

342. Plaintiffs reallege and incorporate by reference all of the above paragraphs, as if fully set forth herein. This claim is pleaded in the alternative to the breach of contractual duty claim.

343. Plaintiffs and members of the Class conferred a benefit upon Defendants in providing Sensitive Information to Defendants.

344. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and the Class. Defendants also benefited from the receipt of Plaintiffs' and the Class's Sensitive Information, as this was used to facilitate the treatment, services, and goods they sold to Plaintiffs and the Class.

345. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs' and the Class's Sensitive Information because Defendants failed to adequately protect their Sensitive Information. Plaintiffs and the proposed Class would not have provided their Sensitive Information to Defendants had they known Defendants would not adequately protect their Sensitive Information.

346. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. Requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

iv. Requiring Defendants to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. Prohibiting Defendants from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. Requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. Requiring Defendants to conduct regular database scanning and securing checks;

xi. Requiring Defendants to establish an information security training program that includes at least annual information security training for all



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. Requiring Defendants to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendants to implement a system of tests to assess their employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting Private Information;

xiv. Requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;



TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

xvi. Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvii. For a period of ten years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, treble, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DATED this 13th day of June, 2025.

Respectfully submitted,

By: *s/ Kaleigh N. Boyd*
Kaleigh N. Boyd, WSBA #52684
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Phone: (206) 682-5600
Fax: (206) 682-2992
kboyd@tousley.com

*Interim Liaison Counsel*

M. Anderson Berry, WSBA #63160
Gregory Haroutunian*
Brandon P. Jack*

CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Email: aberry@justice4you.com

Elena A. Belov
ALMEIDA LAW GROUP LLC
849 W. Webster Ave.
Chicago, Illinois 60614
Telephone: (708) 437-6476
Email: elena@almeidalawgroup.com

*Interim Co-Lead Counsel*

Timothy W. Emery, WSBA #34078
Patrick B. Reddy, WSBA #34092
Brook E. Garberding, WSBA #37140
Paul Cipriani, WSBA #59991
EMERY REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
Telephone: (206) 442-9106
Email: emeryt@emeryreddy.com
Email: reddyp@emeryreddy.com
Email: brook@emeryreddy.com
Email: paul@emeryreddy.com

Samuel J. Strauss, WSBA #46981
Raina Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Telephone: (872) 263-1100
Email: raina@straussborrelli.com

Thomas E. Loeser, WSBA #38701
Karin B. Swope. WSBA #24015
COTCHETT, PITRE & MCCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Telephone: (206)-802-1272
Facsimile: (206)-299-4184
tloeser@cpmlegal.com
kswope@cpmlegal.com

jalhadef@cpmlegal.com

Jeff Ostrow*
Kenneth Grunfeld*
KOPELOWITZ OSTROW P.A.
One W. Las Olas Blvd., Ste. 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com
grunfeld@kolawyers.com

**Pro Hac Vice forthcoming*

*Additional Plaintiffs' Counsel*



**TOUSLEY BRAIN STEPHENS PLLC**
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992