Honorable Barbara J. Rothstein

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

In re Laboratory Services Cooperative Data Breach Litigation	Case No. 2:25-CV-00685-BJR **CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Keyonna Daniels, S.T.[1], Emerald Black, Korri Wynn, Madeline McCann, Cayla Page, Robin Meyabadi, CJ McCurry, N.B., A.B., Keefe John and Tori McMillan ("Plaintiffs"), individually and on behalf of all others similarly situated, state as follows for their consolidated class action complaint against Defendant Laboratory Services Cooperative ("LSC" or "Defendant"):

INTRODUCTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data

[1] Plaintiffs S.T., N.B., and A.B. seek to proceed pseudonymously in this action due to the sensitive nature of the Data Breach. They have already provided their actual identities to Defendant and its counsel with an agreement to keep their identities confidential.

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

Breach").

2. The Data Breach was discovered by Defendant on October 27, 2024. Due to Defendant's failure to implement and follow robust protections necessary to prevent disclosure of highly sensitive information such as medical diagnosis and history, medical treatment, patient names and record numbers, financial information, social security numbers, drivers' license, Defendant enabled criminals to exfiltrate and view its current and former patients' highly personal information, including:

- Social Security Number, driver's license or state ID number, passport number, date of birth, demographic data, student ID number, and other forms of government identifiers, insurance information;
- Billing, claims, and payment data such as claim numbers, bank account details, billing details, billing codes, payment card details, balance details, and other banking and financial information; (both categories together referred to as "personally identifying information" or "PII"); and
- medical diagnosis, treatment, medical record number, lab results, patient number, provider name, treatment location, provider names, health insurance information, and related care details (collectively, "protected health information" or "PHI"). Plaintiffs refer to both PII and PHI collectively as "Sensitive Information."

3. LSC's Data Breach differs from typical data breaches because it affects patients who had no relationship with LSC, never sought one, and never consented to LSC collecting and storing their information.

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

4. LSC sourced Sensitive Information from third parties, including Planned Parenthood, stored that information on LSC's systems, and assumed a duty to protect it. LSC, however, never implemented the security safeguards needed to protect this information despite understanding the importance of the Sensitive Information.

5. On or around April 10, 2025—six months after the Data Breach was first discovered—LSC finally began notifying Class Members about the Data Breach ("Breach Notice"). A sample of the Breach Notice is attached as Exhibit A. However, notice is ongoing, with many Class Members, including some Plaintiffs, still awaiting their formal notice.

6. Due to obfuscating language proffered by LSC, it is unclear when the Data Breach actually took place and how long cybercriminals had unfettered access to Plaintiffs' and the Class's Sensitive Information.

7. The injury to Plaintiffs and Class Members is compounded by the fact that LSC took at least six months before informing *some* Class Members that their Sensitive Information was exposed in the Data Breach, even though Plaintiffs and 1.6 million other Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses, including in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

8. LSC's failure to timely notify the victims of its Data Brach prevented Plaintiffs and Class Members from taking swift and affirmative measures to prevent and mitigate the resulting harm, including but not limited to changing their passwords online to their financial and health-related accounts, and delayed their monitoring for unauthorized activity. When LSC's Breach Notice finally came out, it downplayed the nature of the breach and the threat it posted, providing incomplete information about the Data Breach and refusing to tell its patients when the Data

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

Breach occurred, how many people were impacted, how the breach happened, and why it took Defendant until April 2025 to begin notifying victims that hackers had gained access to highly private Sensitive Information.

9. Defendant's failure to timely detect and report the Data Breach made its patients vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

10. Defendant knew or should have known that each victim of the Data Breach deserved prompt, accurate and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

11. In failing to adequately protect Plaintiffs' and the Class's Sensitive Information, failing to adequately notify them about the Data Breach, and by obfuscating the nature of the Data Breach, Defendant violated state and federal law and harmed an unknown number of its current and former patients and prospective patients.

12. This Data Breach was both foreseeable and preventable. Had LSC followed well-established guidance from many government agencies (e.g., the FTC, Government Accountability Office, as well as others) to take simple but necessary steps to protect Plaintiffs and Class Members' Sensitive Information—such as encrypting sensitive data, minimizing retention periods, enabling multi-factor authentication and access controls, regularly monitoring systems for suspicious activity, setting controls against extractions of large amounts of data, auditing its cybersecurity measures, providing training to its employees, requiring and regularly changing passwords of its employees and vendors—the Data Breach could have been avoided and prevented.

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

13. The security of Plaintiffs and Class Members' identities is at substantial risk because their Sensitive Information is now in the hands of dangerous criminals. This risk will continue for the course of Plaintiffs and Class Members' lives. Defendant exposed Plaintiffs and Class Members to present and imminent risk of fraud and identity theft. Among other measures, Plaintiffs and Class Members already have and will continue to be forced to closely monitor their financial accounts to guard against identity theft. Armed with the Sensitive Information accessed in the Data Breach, data thieves can commit a wide range of crimes.

14. Plaintiffs are current and former patients of healthcare providers to which LSC provides its lab testing services.

15. Accordingly, Plaintiffs, on behalf of themselves and a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

16. Plaintiff Keyonna Daniels is a natural person and a resident and citizen of Sacramento, California.

17. Plaintiff S.T. is a natural person and a resident and citizen of Hawaiian Gardens, California.

18. Plaintiff Emerald Black is a natural person and a resident and citizen of Villejo, California.

19. Plaintiff Korri Wynn is a natural person and a resident and citizen of Baltimore, Maryland.

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

20. Plaintiff Madeline McCann is a natural person and a resident and citizen of Trumansburg, New York.

21. Plaintiff Cayla Page is a natural person and a resident and citizen of Steger, Illinois.

22. Plaintiff Robin Meyabadi is a natural person and a resident and citizen of Lakewood, California.

23. Plaintiff CJ McCurry is a natural person and a resident and citizen of St. Louis, Missouri.

24. Plaintiff N.B. is a natural person and a resident and citizen of Chico, California.

25. Plaintiff A.B. is a natural person and a resident and citizen of San Diego, California.

26. Plaintiff Keefe John is a natural person and a resident and citizen of West Bend, Wisconsin.

27. Plaintiff Tori McMillan is a natural person and a resident and citizen of Renton, Washington.

28. Defendant Laboratory Services Cooperative is a Washington corporation, with its principal place of business at 2001 E Madison Street, Seattle, Washington, 98122-2959.

JURISDICTION AND VENUE

29. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs and Defendant are citizens of different states, and there are over 100 putative Class members.

30. This Court has personal jurisdiction over Defendant because it is headquartered in Washington, regularly conducts business in Washington, and has sufficient minimum contacts in Washington.

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

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

STATEMENT OF FACTS

Background on LSC

32. LSC is a Washington state-based diagnostic testing services provider."[2] Defendant boasts a total annual revenue of approximately $18 million.[3]

33. As part of its business, Defendant receives and maintains the Sensitive Information of thousands of patients (such as, *inter alia*, its clients' patients). In collecting and maintaining Sensitive Information, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class members themselves took reasonable steps to secure their Sensitive Information.

34. Despite recognizing its duty to do so, on information and belief, LSC has not implemented reasonable cybersecurity safeguards or policies to protect its patients' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, LSC leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Sensitive Information.

The Data Breach

35. On information and belief, Defendant collects and maintains patients' Sensitive Information in its computer systems.

---

[2] SC Media, https://www.scworld.com/brief/attack-against-laboratory-services-cooperative-impacts-1-6m (last visited Apr. 16, 2025).

[3] ProPublica, https://projects.propublica.org/nonprofits/organizations/263813271 (last visited Apr. 16, 2025).

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

36. In collecting and maintaining Sensitive Information, Defendant implicitly agrees that it will safeguard the data using reasonable means according to state and federal law.

37. According to its Breach Notice, on October 27, 2024, Defendant was alerted that "LSC identified suspicious activity within its network." Ex. A. Following an internal investigation, Defendant confirmed that "certain LSC patient and worker-related data" had been affected by the unauthorized actor. *Id.*

38. In other words, Defendant's cyber and data security systems were so completely inadequate that it allowed cybercriminals to obtain files containing a treasure trove of thousands of its patients' highly private Sensitive Information.

39. Through its inadequate security practices, Defendant exposed Plaintiffs' and the Class's Sensitive Information for theft and sale on the dark web.

40. On or around April 10, 2025—six months after the Breach was discovered—LSC finally began notifying Class Members about the Data Breach. However, notification is ongoing and many Class Members, including some Plaintiffs, have yet to receive formal notice.

41. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendant did not follow industry standard practices in securing patients' Sensitive Information, as evidenced by the Data Breach.

42. Typically, in response to a data breach, a company will promise to implement enhancement and additional cybersecurity steps to prevent a similar breach from occurring again. Not Defendant. Instead, Defendant placed the onus on Plaintiffs and the Class, informing them to regularly review their accounts and credit reports for instances of fraud and identity theft caused by Defendant's inadequate cybersecurity.

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

43. In its Breach Notice, Defendant also recognized and acknowledged the actual imminent harm and injury to Class members that flowed from the Data Breach, as it encouraged breach victims to be "vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity." Ex. A.

44. In its Breach Notice, Defendant further recognized its duty to provide adequate cybersecurity, insisting that, despite the Data Breach demonstrating otherwise, "[t]he confidentiality, privacy, and security of information maintained by LSC remains its top priority." Ex. A.

45. Cybercriminals need not harvest a person's Social Security number or financial account information to commit identity fraud or misuse Plaintiffs' and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

46. On information and belief, LSC has offered several months of complimentary credit monitoring services to some victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the Data Breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

47. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

48. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement

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

reasonable security measures, causing it to lose control over its patients' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

49. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare and healthcare adjacent industry preceding the date of the breach.

50. In light of recent high-profile data breaches at other healthcare and healthcare adjacent companies, Defendant knew or should have known that its electronic records and patients' Sensitive Information would be targeted by cybercriminals.

51. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[4] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[5]

52. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[6]

---

[4] *2021 in Review: Data Breach Annual Report*, ITRC, https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited July 2, 2025).

[5] *Id.*

[6] Gordon M. Snow Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

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

53. Cyberattacks on medical systems and healthcare and healthcare adjacent companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[7]

54. In fact, many high-profile ransomware attacks have occurred in healthcare and healthcare adjacent companies, with an estimate that nearly half of all ransomware attacks being carried out are on healthcare companies and 85% of those attacks being ransomware similar to the attack here.[8]

55. Therefore, the increase in such attacks, and attendant risk of future attacks, were widely known to the public and to anyone in Defendant's industry, including Defendant.

Plaintiff Keyonna Daniels' Experience

56. As a condition of receiving services from Planned Parenthood, Plaintiff Daniels was required to provide her PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

57. Plaintiff Daniels' PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of this Data Breach, even though Plaintiff Daniels did not otherwise have any connection to LSC.

[7] *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[8] *Ransomware explained: How it works and how to remove it*, CSO (Oct. 2, 2024), https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

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

58. Plaintiff Daniels greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Daniels took reasonable steps to maintain the confidentiality of her PII and PHI.

59. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff Daniels was never individually notified of the Data Breach.

60. Since learning of the Data Breach, Plaintiff Daniels has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent researching the Data Breach, time spent self-monitoring her accounts and credit, and time spent worrying about her PII and PHI being exposed, all as a result of her PII and PHI being exposed in the Data Breach. Since April 2024, she has spent approximately one hour per week monitoring her accounts and credit as a result of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff Daniels intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

61. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Daniels would take, and continue to take, necessary measures to protect her PII and PHI.

62. As a result of the Data Breach, Plaintiff Daniels spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

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

63. In addition, as a result of the Data Breach Plaintiff Daniels has suffered, will continue to suffer, and has increased concerns for the loss of her privacy which she would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred, LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff Daniels.

64. Plaintiff Daniels plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her credit and financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

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

66. Plaintiff Daniels has a continuing interest in ensuring that her Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

67. Plaintiff Daniels has suffered actual, concrete injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and

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

opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

68. Plaintiff Daniels has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of her PII and PHI, especially her PII and PHI from Planned Parenthood, along with her sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

69. As a direct and traceable result of the Data Breach, Plaintiff Daniels will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff S.T. Experience

70. As a condition of receiving services from Planned Parenthood, Plaintiff S.T. was required to provide her PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

71. Plaintiff S.T.'s PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of its Data Breach, even though Plaintiff S.T. did not otherwise have any connection to LSC.

72. Plaintiff S.T. greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff S.T. took reasonable steps to maintain the confidentiality of her PII and PHI.

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

73. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff S.T. was not individually notified of the Data Breach at all.

74. Since learning of the Data Breach, Plaintiff S.T. has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent researching the Data Breach, time spent self-monitoring her accounts, and time spent worrying about her PII and PHI related to Planned Parenthood being exposed, all as a result of her PII and PHI being exposed in the Data Breach. Since April 2025, she has spent approximately 2 hours dealing with the consequences of the Data Breach. In the Breach Notice on LSC's website, LSC directed affected individuals like Plaintiff to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff S.T. intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

75. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff S.T. would take, and continue to take, necessary measures to protect her PII and PHI.

76. As a result of the Data Breach, Plaintiff S.T. spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

77. In addition, as a result of the Data Breach Plaintiff S.T. has suffered, will continue to suffer, and has increased concerns for the loss of her privacy which she would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from

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

theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred, LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff at all.

78. Plaintiff S.T. plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

79. Additionally, Plaintiff S.T. is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source.

80. Plaintiff S.T. has a continuing interest in ensuring that her Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

81. Plaintiff S.T. has suffered actual, concrete injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

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

82. Plaintiff S.T. has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of his/her PII and PHI, especially her PII from Planned Parenthood, along with her sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

83. As a direct and traceable result of the Data Breach, Plaintiff S.T. will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Emerald Black's Experience

84. As a condition of receiving services from Planned Parenthood, Plaintiff Black was required to provide her PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

85. Plaintiff Black's PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of its Data Breach, even though Plaintiff Black did not otherwise have any connection to LSC.

86. Plaintiff Black greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Black took reasonable steps to maintain the confidentiality of her PII and PHI.

87. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff Black was not individually notified of the Data Breach at all.

88. After the Data Breach, Plaintiff experienced an increase in suspicious spam calls and emails, including an increase in phishing attempts.

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

89. Since learning of the Data Breach, Plaintiff Black has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent researching the Data Breach, time spent self-monitoring her accounts, and time spent worrying about her PII and PHI related to Planned Parenthood being exposed, all as a result of her PII and PHI being exposed in the Data Breach. Since April 2025, she has spent approximately 8–10 hours dealing with the consequences of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals like Plaintiff to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff Black intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

90. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Black would take, and continue to take, necessary measures to protect her PII and PHI.

91. As a result of the Data Breach, Plaintiff Black spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

92. In addition, as a result of the Data Breach Plaintiff Black has suffered, will continue to suffer, and has increased concerns for the loss of her privacy which she would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred,

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

LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff at all.

93. Plaintiff Black plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

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

95. Plaintiff Black has a continuing interest in ensuring that her Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI it keeps.

96. Plaintiff Black has suffered actual, concrete injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

97. Plaintiff Black has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from

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

the compromise of her PII and PHI, especially her PII from Planned Parenthood, along with her sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

98. As a direct and traceable result of the Data Breach, Plaintiff Black will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Korri Wynn's Experience

99. As a condition of receiving services from Planned Parenthood, Plaintiff Wynn was required to provide her PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

100. Plaintiff Wynn's PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of its Data Breach, even though Plaintiff Wynn did not otherwise have any connection to LSC.

101. Plaintiff Wynn greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Wynn took reasonable steps to maintain the confidentiality of her PII and PHI.

102. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff Wynn was never individually notified of the Data Breach.

103. After the Data Breach, Plaintiff Wynn experienced a significant increase in spam calls and text messages, some of which leave voicemails that reference Planned Parenthood. As a result, she had to adjust her phone settings so that unknown callers go straight to voicemail, as a mechanism for screening her calls.

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

104. Since learning of the Data Breach, Plaintiff Wynn has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent learning about the Data Breach, time spent filtering through unwanted spam calls and text messages, and time spent worrying about her PII and PHI being exposed, all as a result of her PII and PHI being exposed in the Data Breach. Since the Data Breach, she has spent approximately five minutes each day dealing with the consequences of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff Wynn intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

105. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Wynn would take, and continue to take, necessary measures to protect her PII and PHI.

106. As a result of the Data Breach, Plaintiff Wynn spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

107. In addition, as a result of the Data Breach Plaintiff Wynn has suffered, will continue to suffer, and has increased concerns for the loss of her privacy which she would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred,

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

LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff Wynn.

108. Plaintiff Wynn plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, filtering spam calls and text messages, and addressing any issues that may arise.

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

110. Plaintiff Wynn has a continuing interest in ensuring that her Sensitive Information, which remain in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

111. Plaintiff Wynn has suffered actual, concrete injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

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

112. Plaintiff Wynn has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of her PII and PHI, especially her PII and PHI from Planned Parenthood, along with her sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

113. As a direct and traceable result of the Data Breach, Plaintiff Wynn will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Madeline McCann's Experience

114. As a condition of receiving services from Planned Parenthood, Plaintiff McCann was required to provide her PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

115. Plaintiff McCann's PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of its Data Breach, even though Plaintiff McCann did not otherwise have any connection to LSC.

116. Plaintiff McCann greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff McCann took reasonable steps to maintain the confidentiality of her PII and PHI.

117. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff McCann was not individually notified of the Data Breach at all.

118. Since learning of the Data Breach, Plaintiff McCann has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the

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

Data Breach, including time spent researching the Data Breach and consulting with family and friends, time spent monitoring her accounts, and time spent worrying about her PII and PHI related to Planned Parenthood being exposed, all as a result of her PII and PHI being exposed in the Data Breach. Since April 2025, she has spent approximately 3-4 hours dealing with the consequences of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals like Plaintiff to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff McCann intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

119. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff McCann would take, and continue to take, necessary measures to protect her PII and PHI.

120. As a result of the Data Breach, Plaintiff McCann spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

121. In addition, as a result of the Data Breach Plaintiff McCann has suffered, will continue to suffer, and has increased concerns for the loss of her privacy which she would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred, LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff at all.

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

122. Plaintiff McCann plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

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

124. Plaintiff McCann has a continuing interest in ensuring that her Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

125. Plaintiff McCann has suffered actual, concrete injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

126. Plaintiff McCann has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of her PII and PHI, especially her PII from Planned Parenthood, along with her

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

sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

127. As a direct and traceable result of the Data Breach, Plaintiff McCann will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Cayla Page's Experience

128. As a condition of receiving services from Planned Parenthood, Plaintiff Page was required to provide her PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

129. Plaintiff Page's PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of its Data Breach, even though Plaintiff Page did not otherwise have any connection to LSC.

130. Plaintiff Page greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Page took reasonable steps to maintain the confidentiality of her PII and PHI.

131. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff Page was never individually notified of the Data Breach.

132. After the Data Breach, Plaintiff Page was notified that her personal information had been discovered on the dark web and that her passwords for various accounts had been compromised.

133. In December 2024, Plaintiff Page experienced fraudulent charges on her Chase account, the same account she would have used to make any payments to Planned Parenthood. As

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

a result, Plaintiff had to obtain a new payment card associated with the account and drove to the bank in an effort to obtain the new payment card. She also had to reset her Chase account automatic billing instructions.

134. In December of 2024, after the Data Breach, Plaintiff Page was informed of certain issues with her credit when she applied for a loan.

135. Since the Data Breach, Plaintiff has also experienced a significant increase in spam text messages.

136. Since learning of the Data Breach, Plaintiff Page has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent researching the Data Breach, self-monitoring her accounts, disputing fraudulent bank charges, and driving to the bank to obtain a new banking card, as well as time spent worrying about her PII and PHI being exposed, all as a result of her PII and PHI being exposed in the Data Breach. Since the Data Breach, she has spent approximately four hours dealing with the consequences of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff Page intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

137. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Page would take, and continue to take, necessary measures to protect her PII and PHI.

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

138. As a result of the Data Breach, Plaintiff Page spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

139. In addition, as a result of the Data Breach Plaintiff Page has suffered, will continue to suffer, and has increased concerns for the loss of her privacy which she would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred, LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff Page.

140. Plaintiff Page plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

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

142. Plaintiff Page has a continuing interest in ensuring that her Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

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

143. Plaintiff Page has suffered actual, concrete injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

144. Plaintiff Page has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of her PII and PHI, especially her PII and PHI from Planned Parenthood, along with her sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

145. As a direct and traceable result of the Data Breach, Plaintiff Page will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Robin Meyabadi's Experience

146. As a condition of receiving services from Planned Parenthood, Plaintiff Meyabadi was required to provide her PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

147. Plaintiff Meyabadi's PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of its Data Breach, even though Plaintiff Meyabadi did not otherwise have any connection to LSC.

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

148. Plaintiff Meyabadi greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Meyabadi took reasonable steps to maintain the confidentiality of her PII and PHI.

149. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff Meyabadi was never individually notified of the Data Breach.

150. After the Data Breach, Plaintiff Meyabadi received notification from one of her credit monitoring services that her personal information was found on the dark web.

151. Since the Data Breach, Plaintiff Meyabadi has also experienced an increase in spam calls and text messages.

152. Since learning of the Data Breach, Plaintiff Meyabadi has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent researching the Data Breach, time spent self-monitoring her accounts, and time spent worrying about her PII and PHI being exposed, all as a result of her PII and PHI being exposed in the Data Breach. Since the Data Breach, she has spent several hours dealing with the consequences of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff Meyabadi intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

153. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Meyabadi would take, and continue to take, necessary measures to protect her PII and PHI.

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

154. As a result of the Data Breach, Plaintiff Meyabadi spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

155. Plaintiff Meyabadi plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

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

157. Plaintiff Meyabadi has a continuing interest in ensuring that her Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

158. Plaintiff Meyabadi has suffered actual, concrete injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI.

159. Plaintiff Meyabadi has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from

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

the compromise of her PII and PHI, especially her PII and PHI from Planned Parenthood, along with her sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

160. As a direct and traceable result of the Data Breach, Plaintiff Meyabadi will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff CJ McCurry's Experience

161. As a condition of receiving services from Planned Parenthood, Plaintiff McCurry was required to provide his PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

162. Plaintiff McCurry's PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of its Data Breach, even though Plaintiff McCurry did not otherwise have any connection to LSC.

163. Plaintiff McCurry greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff McCurry took reasonable steps to maintain the confidentiality of his PII and PHI.

164. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff McCurry was never individually notified of the Data Breach.

165. After the Data Breach, Plaintiff experienced an increase in spam calls related to medical inquiries.

166. Since learning of the Data Breach, Plaintiff McCurry has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the

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

Data Breach, including time spent researching the Data Breach and self-monitoring his accounts, all as a result of his PII and PHI being exposed in the Data Breach. Since the Data Breach, he has spent approximately 10 hours dealing with the consequences of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff McCurry intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

167. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff McCurry would take, and continue to take, necessary measures to protect his PII and PHI.

168. As a result of the Data Breach, Plaintiff McCurry spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

169. In addition, as a result of the Data Breach Plaintiff McCurry has suffered, will continue to suffer, and has increased concerns for the loss of his privacy which he would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred, LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff McCurry.

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

170. Plaintiff McCurry plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

171. Additionally, Plaintiff McCurry is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff McCurry stores any documents containing his PII or PHI in a safe and secure location or destroys the documents.

172. Plaintiff McCurry has a continuing interest in ensuring that his Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

173. Plaintiff McCurry has suffered actual, concrete injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of his PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

174. Plaintiff McCurry has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from the compromise of his PII and PHI, especially his PII and PHI from Planned Parenthood, along

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

with his sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

175. As a direct and traceable result of the Data Breach, Plaintiff McCurry will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff N.B.'s Experience

176. As a condition of receiving services from Planned Parenthood, Plaintiff N.B. was required to provide her PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

177. Plaintiff N.B.'s PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of its Data Breach, even though Plaintiff N.B. did not otherwise have any connection to LSC.

178. Plaintiff N.B. greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff N.B. took reasonable steps to maintain the confidentiality of her PII and PHI.

179. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff was never individually notified of the Data Breach.

180. Since learning of the Data Breach, Plaintiff N.B. has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent researching the Data Breach, time spent monitoring her accounts, and time spent worrying about her PII and PHI related to Planned Parenthood being exposed, all as a result of her PII and PHI being exposed in the Data Breach. Since April 2025, she has spent

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

approximately 3 hours dealing with the consequences of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals like Plaintiff to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff N.B. intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

181. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff N.B. would take, and continue to take, necessary measures to protect her PII and PHI.

182. As a result of the Data Breach, Plaintiff N.B. spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

183. In addition, as a result of the Data Breach Plaintiff N.B. has suffered, will continue to suffer, and has increased concerns for the loss of her privacy which she would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred, LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff at all.

184. Plaintiff N.B. plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

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

185. Additionally, Plaintiff N.B. is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source.

186. Plaintiff N.B. has a continuing interest in ensuring that her Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

187. Plaintiff N.B. has suffered actual, concrete injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

188. Plaintiff N.B. has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of his/her PII and PHI, especially her PII from Planned Parenthood, along with her sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

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

189. As a direct and traceable result of the Data Breach, Plaintiff N.B. will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff A.B.'s Experience

190. As a condition of receiving services from Planned Parenthood, Plaintiff A.B. was required to provide her PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

191. Plaintiff A.B.'s. PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of its Data Breach, even though Plaintiff A.B. did not otherwise have any connection to LSC.

192. Plaintiff A.B. greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff A.B. took reasonable steps to maintain the confidentiality of her PII and PHI.

193. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff A.B. was not individually notified of the Data Breach.

194. After the Data Breach, Plaintiff experienced an increase in suspicious spam calls, emails, and text messages.

195. Since learning of the Data Breach, Plaintiff A.B. has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent researching the Data Breach, considering credit monitoring and identity theft insurance options, self-monitoring her accounts, and opening a new credit card and new bank account, all as a result of her PII and PHI being exposed in the Data Breach. Since April

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

2025, she has spent approximately 6 hours dealing with the consequences of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals to spend time mitigating his losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff A.B. intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

196. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff A.B. would take, and continue to take, necessary measures to protect her PII and PHI.

197. As a result of the Data Breach, Plaintiff A.B. spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

198. In addition, as a result of the Data Breach Plaintiff A.B. has suffered, will continue to suffer, and has increased concerns for the loss of her privacy which she would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred, LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff at all.

199. Plaintiff A.B. plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

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

200. Additionally, Plaintiff A.B. is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source.

201. Plaintiff A.B. has a continuing interest in ensuring that her Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

202. Plaintiff A.B. has suffered actual, concrete injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

203. Plaintiff A.B. has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of his/her PII and PHI, which are now in the hands of cybercriminals and other unauthorized third parties.

204. As a direct and traceable result of the Data Breach, Plaintiff A.B. will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, 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 Keefe John's Experience

205. As a condition of receiving services from Planned Parenthood, Plaintiff John was required to provide his PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

206. Plaintiff John's PII and PHI from Planned Parenthood was, on information and belief, provided to LSC and became part of its Data Breach, even though Plaintiff John did not otherwise have any connection to LSC.

207. Plaintiff John greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff John took reasonable steps to maintain the confidentiality of his PII and PHI.

208. Plaintiff John did not receive any notice of the Data Breach from LSC but when he contacted the Data Breach hotline, he was informed that his PII and PHI were part of the Data Breach.

209. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025.

210. Since learning of the Data Breach, Plaintiff John has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent researching the Data Breach and self-monitoring his accounts, all as a result of his PII and PHI being exposed in the Data Breach. Since the Data Breach, he has spent several hours dealing with the consequences of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff John intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

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

211. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff John would take, and continue to take, necessary measures to protect his PII and PHI.

212. As a result of the Data Breach, Plaintiff John spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

213. In addition, as a result of the Data Breach Plaintiff John has suffered, will continue to suffer, and has increased concerns for the loss of his privacy which he would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred, LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff John.

214. Plaintiff John plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

215. Additionally, Plaintiff John is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source.

216. Plaintiff John has a continuing interest in ensuring that his Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for

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

unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

217. Plaintiff John has suffered actual, concrete injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of his PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

218. Plaintiff John has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from the compromise of his PII and PHI, especially his PII and PHI from Planned Parenthood, along with his sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

219. As a direct and traceable result of the Data Breach, Plaintiff John will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Tori McMillan's Experience

220. As a condition of receiving services from Planned Parenthood, Plaintiff McMillan was required to provide her PII and PHI, which was then obtained by LSC, entered into LSC's database, and maintained by LSC.

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

221. Plaintiff McMillan's PII and PHI from Planned Parenthood was, on information and belief, transferred to LSC and became part of its Data Breach, even though Plaintiff McMillan did not otherwise have any connection to LSC.

222. Plaintiff McMillan greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff McMillan took reasonable steps to maintain the confidentiality of her PII and PHI.

223. Plaintiff McMillan only discovered that she was impacted by the Data Breach by contacting LSC (via the Data Breach notification phone number). She did not receive any written notice of the Data Breach from LSC.

224. Although LSC discovered the Data Breach in October 2024, the general public was not notified of the Data Breach until in or around April 2025, and Plaintiff McMillan was never individually notified of the Data Breach.

225. After the Data Breach, Plaintiff McMillan experienced a significant increase in spam calls (up to four calls a day), text messages, and email communications.

226. Since learning of the Data Breach, Plaintiff McMillan has spent additional time reaching out to LSC to confirm her PII and PHI was impacted and dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent researching the Data Breach, screening spam phone calls and text messages, filtering spam emails, considering credit monitoring and identity theft insurance options, self-monitoring her accounts, worrying about her personal information being exposed, and looking for, and considering other health provider options, all as a result of her PII and PHI being exposed in the Data Breach. Since the Data Breach, she has spent approximately sixteen hours dealing with the consequences of the Data Breach. In the Breach Notice posted on LSC's website, LSC directed all affected individuals

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

to spend time mitigating their losses by "regularly reviewing your accounts and monitoring credit reports for suspicious activity." Plaintiff McMillan intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

227. Moreover, the PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff McMillan would take, and continue to take, necessary measures to protect her PII and PHI.

228. As a result of the Data Breach, Plaintiff McMillan spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

229. In addition, as a result of the Data Breach Plaintiff McMillan has suffered, will continue to suffer, and has increased concerns for the loss of her privacy which she would not have incurred had LSC implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that LSC has not been forthright with information about the Data Breach, the manner in which the breach occurred, LSC's failure to notify the public for over five months, and LSC's failure to individually notify impacted individuals like Plaintiff McMillan.

230. Plaintiff McMillan plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, screening and filtering spam calls, text messages, and emails, and addressing any issues that may arise.

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

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

232. Plaintiff McMillan has a continuing interest in ensuring that her Sensitive Information, which remains in Defendant's possession, is protected and safeguarded from future breaches. Upon information and belief, Plaintiff's PII and PHI: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

233. Plaintiff McMillan has suffered actual, concrete injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII and PHI. Plaintiff also has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

234. Plaintiff McMillan has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of her PII and PHI, especially her PII and PHI from Planned Parenthood along with her other sensitive health information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

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

235. As a direct and traceable result of the Data Breach, Plaintiff McMillan will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

236. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

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

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

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

238. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

239. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

240. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

241. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

242. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

243. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class' 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 Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including

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

this Court or a jury, to find that Plaintiffs' and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

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

245. Defendant's failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Failed to Adhere to FTC Guidelines

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

247. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

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

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

249. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

251. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

252. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly

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

known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [9]

253. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[10]

254. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or

[9] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[10] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

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

software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

255. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Consumers Prioritize Data Security

256. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[11] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a

[11] *Privacy Awareness: Consumers Taking Charge to Protect Personal Information*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited July 2, 2025).

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

customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[12]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[13]

c. 89% of consumers stated that "I care about data privacy."[14]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[15]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[16]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[17]

257. Defendant knew or should have known that adequate implementation of cybersecurity and protection of Sensitive Information, including Plaintiffs and the Class's Sensitive Information was important to its client's patients, and should have implemented adequate cybersecurity measures to protect the Sensitive Information. Yet, Defendant failed to do so.

Defendant Failed to Comply with Industry Standards

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

---

[12] *Id.* at 3.
[13] Id.
[14] *Id.* at 9.
[15] Id.
[16] Id.
[17] *Id.* at 11.

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

259. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

260. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

261. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 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).

262. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—if not all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

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

CLASS ACTION ALLEGATIONS

263. Plaintiffs are suing on behalf of themselves and the proposed Nationwide Class ("Class") and Subclasses, defined as follows:

> **Nationwide Class:** All US citizens whose Sensitive Information was compromised in the Data Breach discovered by Defendant in June 2024, including all those citizens who received notice of the breach.
>
> **California Subclass:** All California citizens whose Sensitive Information was compromised in the Data Breach discovered by Defendant in June 2024, including all those citizens who received notice of the breach.
>
> **Washington Subclass:** All Washington citizens whose Sensitive Information was compromised in the Data Breach discovered by Defendant in June 2024, including all those citizens who received notice of the breach.
>
> **Illinois Subclass:** All Illinois citizens whose Sensitive Information was compromised in the Data Breach discovered by Defendant in June 2024, including all those citizens who received notice of the breach.
>
> **New York Subclass:** All New York citizens whose Sensitive Information was compromised in the Data Breach discovered by Defendant in June 2024, including all those citizens who received notice of the breach.

264. Excluded from the Class and Subclasses are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

265. Plaintiffs reserve the right to amend the class definition.

266. **Numerosity**. Plaintiffs are representatives of the Class and Subclasses, consisting of several thousands of members, far too many to join in a single action;

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

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

268. **Typicality**. As to the Class and each Subclass, Plaintiffs' claims are typical of the class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

269. **Adequacy**. Plaintiffs will fairly and adequately protect the interests of the proposed Class and Subclasses. Their interests do not conflict with the Class's interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

270. **Commonality**. As to the Class and each Subclass, Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Sensitive Information;

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

iii. Whether Defendant were negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's Sensitive Information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

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

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

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

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

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

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

274. Defendant accepted possession of Plaintiffs' and Class Members' Sensitive Information for the purpose of performing its regular business operations.

275. Defendant owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Sensitive Information in a data breach. And here, that foreseeable danger came to pass.

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

276. Defendant has full knowledge of the sensitivity of the Sensitive Information and the types of harm that Plaintiffs and the Class could and would suffer if their Sensitive Information was wrongfully disclosed.

277. Defendant's act of collecting, retaining, and storing Plaintiffs' and Class Members' PII and PHI constitutes an affirmative act that created a high degree of risk that third parties would attempt to obtain the personal information.

278. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs' and Class members' Sensitive Information.

279. Defendant owed—to Plaintiffs and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the Sensitive Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their Sensitive Information.

280. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their

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

Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

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

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

283. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Sensitive Information, a necessary part of obtaining services from Defendant.

284. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Sensitive Information.

285. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the Sensitive Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the Class members' sensitive Information.

286. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given

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

the nature and amount of Sensitive Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

287. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiffs' and Class members' PHI.

288. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed supra. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

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

290. Sensitive Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiffs and Class members and the importance of exercising reasonable care in handling it. Despite the widespread knowledge of the risks of inadequately securing PHI and PII, Defendant designed and implemented its systems with inadequate safety and security protocol, leaving its systems vulnerable to access by unauthorized users.

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

291. Defendant improperly and inadequately safeguarded the Sensitive Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

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

293. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' Sensitive Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

294. Defendant breached its duties by failing to exercise reasonable care in designing and implementing its IT systems and controls; in supervising its agents, contractors, vendors, and suppliers; and in handling and securing the personal information and Sensitive Information of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs' and Class members' injury.

295. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class members' injuries-in-fact.

296. Defendant has admitted that the Sensitive Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

297. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages, including

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

monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

298. And, on information and belief, Plaintiffs' Sensitive Information has already been published—or will be published imminently—by cybercriminals on the dark web.

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

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

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

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

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

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

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

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

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

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

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

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

308. This claim is pleaded in the alternative to the breach of contractual duty claim.

309. Plaintiffs and members of the Class (or their third-party agents) conferred a benefit upon Defendant in providing Sensitive Information to Defendant.

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

311. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs and the Class's Sensitive Information because Defendant failed

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

to adequately protect their Sensitive Information. Plaintiffs and the proposed Class would not have provided their Sensitive Information to Defendant had they known Defendant would not adequately protect their Sensitive Information.

312. Defendant 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.

COUNT IV
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

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

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

315. Defendant owed a duty to its client's current and former patients, including Plaintiffs and the Class, to keep this information confidential.

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

317. 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 Defendant, but 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.

318. 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

319. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

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

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

322. As a proximate result of Defendant's acts and omissions, the private 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 (as detailed supra).

323. And, on information and belief, Plaintiffs' Sensitive Information has already been published—or will be published imminently—by cybercriminals on the dark web.

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

325. 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 Defendant's inability to safeguard the Sensitive Information of Plaintiffs and the Class.

326. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seek compensatory damages for Defendant's invasion of privacy, which

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

includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT V
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiffs and the Class)

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

328. The Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., authorizes this Court to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

329. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

330. Defendant owes a duty of care to Plaintiffs and Class Members which require it to adequately secure its Sensitive Information when it chose to accept and store Plaintiffs' and Class Members' Sensitive Information.

331. Defendant still possesses Plaintiffs' and Class Members' Sensitive Information.

332. Defendant does not specify in the Data Breach notification posted on its website what specific and verifiable steps it has taken to prevent a similar breach from occurring again.

333. Plaintiffs and Class Members are at risk of harm due to the exposure of their Sensitive Information and the Defendant's failures to address the security failings that led to such exposure.

334. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Sensitive Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their Sensitive Information.

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

335. Plaintiffs and the Class, therefore, seek a declaration that (1) each of Defendant's existing security measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect consumers' Sensitive Information, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's utter failure to provide notice to all affected consumers);

b. Requiring Defendant to implement adequate security protocols and practices to protect consumers' Sensitive Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

c. Mandating the proper notice be sent to all affected consumers, and posted publicly;

d. Requiring Defendant to protect all data collected through any manner;

e. Requiring Defendant to delete, destroy, and purge the Sensitive Information of Plaintiffs and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

f. Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Sensitive Information;

g. Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

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

h. Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

i. Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

j. Requiring Defendant to conduct systematic scanning for data breach related issues;

k. Requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the Sensitive Information; and

l. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

336. The Court can, and should, issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with the law and industry standards to protect Plaintiffs' and Class Members' Sensitive Information.

337. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of the Defendant's systems or networks. The risk of another breach is real, immediate, and substantial.

338. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs, the Plaintiffs and the Class will likely be subjected to fraud, identity theft, and other harms described herein. However, the cost to the Defendant of complying with an injunction by employing reasonable

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

prospective data security measures is minimal given they have preexisting legal obligations to employ these measures.

COUNT VI
Violation of the Washington Consumer Protection Act RCW 19.86
(On Behalf of Plaintiffs and the Class, or in the alternative, the Washington Subclass)

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

340. The Washington State Consumer Protection Act, RCW 19.86.020 (the "WCPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the WCPA and relevant case law.

341. Defendant is a "person" as described in RCW 19.86.010(1).

342. Defendant engages in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the state of Washington.

343. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning of, and in violation of, the WCPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

344. Defendant's failure to safeguard the Sensitive Information exposed in the Data Breach constitutes an unfair act that offends public policy.

345. Defendant's failure to safeguard the Sensitive Information compromised in the Data Breach caused substantial injury to Plaintiffs' and Class Members. Defendant's failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

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

346. Defendant's failure to safeguard the Sensitive Information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, was unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

347. In the course of conducting its business, Defendant committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' Sensitive Information, and violating the common law alleged herein in the process. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

348. Defendant also violated the WCPA by failing to timely notify, and by concealing from Plaintiffs and Class Members, information regarding the unauthorized release and disclosure of their Sensitive Information. If Plaintiffs and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Sensitive Information.

349. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

350. Defendant's unfair or deceptive acts or practices occurred in its trade or business and have injured and are capable of injuring a substantial portion of the public. Defendant's general

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

course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

351. Defendant's unfair or deceptive acts or practices emanated from its headquarters in Washington State and have injured and are capable of injuring a substantial portion of the public across the United States.

352. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the WCPA, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate, and continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) invasion of privacy; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) the financial and temporal costs of monitoring credit, monitoring financial accounts, and mitigating damages.

353. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves and the Class, seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Sensitive Information entrusted to it.

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

354. Plaintiffs, on behalf of themselves and Class Members, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorneys' fees. In addition, Plaintiffs, on behalf of themselves and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained, not to exceed $25,000.00 per Class Member.

COUNT VII
Violation of the California Customer Records Act,
Cal. Civ. Code § 1798.80, et seq.
(On Behalf of Plaintiffs Daniels, S.T., Black, Meyabadi,
N.B., A.B. and the California Subclass)

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

356. Under the California Customer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *Id* (emphasis added).

357. The Data Breach constitutes a "breach of the security system" of Defendant.

358. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the Class.

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

359. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the Class but waited approximately two months to notify them. Given the severity of the Data Breach, six months was an unreasonable delay.

360. Defendant's unreasonable delay prevented Plaintiffs and the Class from taking appropriate measures from protecting themselves against harm.

361. Because Plaintiffs and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

362. Plaintiffs and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT VIII
Violation of California's Unfair Competition Law ("UCL")
Cal Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiffs Daniels, S.T., Black, Meyabadi, N.B., A.B. and the California Subclass)

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

364. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, et seq. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

365. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), and other state data security laws.

366. Defendant stored the Sensitive Information of Plaintiffs and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiffs' and the Class's Sensitive Information secure so as to prevent the loss or misuse of that Sensitive Information.

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

367. Defendant failed to disclose to Plaintiffs and the Class that their Sensitive Information was not secure. However, Plaintiffs and the Class were entitled to assume, and did assume, that Defendant had secured their Sensitive Information. At no time were Plaintiffs and the Class on notice that their Sensitive Information was not secure, which Defendant had a duty to disclose.

368. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and the Class's nonencrypted and nonredacted Sensitive Information.

369. Had Defendant complied with these requirements, Plaintiffs and the Class would not have suffered the damages related to the data breach.

370. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

371. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

372. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting Sensitive Information.

373. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of

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

computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

374. Instead, Defendant made the Sensitive Information of Plaintiffs and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

375. As a result of those unlawful and unfair business practices, Plaintiffs and the Class suffered an injury-in-fact and have lost money or property.

376. The injuries to Plaintiffs and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

377. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

378. Defendant has not yet implemented adequate protections to prevent a future data breach, nor has it given adequate notice to all affected class members, and therefore, the equitable relief requested here would prevent ongoing and future harm;

379. Injunctive relief is also necessary to prevent the members of general public from being misled by Defendant's misrepresentations regarding privacy and security of information;

380. The equitable relief under the UCL creates a straightforward cause of action for violations of law. Furthermore, damages for non-UCL claims require additional elements or pre-

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

suit notice letters, which would potentially eliminate the possibility of providing damages to the entire class, while restitution would provide certainty and remedy for all affected victims.

381. In addition, discovery—which has not yet been provided and/or completed—may reveal that the claims providing legal remedies are inadequate. At this time, forcing an election of remedies at the initial pleadings stage, in the absence of completed discovery regarding class certification and merits, is premature and likely to lead to subsequent, potentially belated, and hotly contested motions to amend the pleadings to add equitable remedies based on a lengthy historical recount of discovery and analysis of voluminous exhibits, transcripts, discovery responses, document productions, etc., as well as related motions to seal confidential information contained therein.

382. Therefore, Plaintiffs and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT IX
Violation of California Consumer Protection Act ("CCPA")
California Civil Code § 1798.150, *et seq.*
(On Behalf of Plaintiffs Daniels, S.T., Black, Meyabadi, N.B., A.B. and the California Subclass)

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

384. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Sensitive Information of Plaintiffs and the Class. As a direct and proximate result, Plaintiffs', and the Class's nonencrypted and nonredacted Sensitive Information was subject to unauthorized access and exfiltration, theft, or disclosure.

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

385. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its customers, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

386. Plaintiffs and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Sensitive Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Sensitive Information, including Plaintiffs' and Class members' Sensitive Information. Plaintiffs and Class members have an interest in ensuring that their Sensitive Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

387. Pursuant to California Civil Code § 1798.150(b), Plaintiffs mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiffs believes such cure is not possible under these facts and circumstances—then Plaintiffs intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

388. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

389. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

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

COUNT X
Violation of the New York General Business Law
N.Y. Gen. Bus. Law *§§ 349, et seq.*
(On Behalf of Plaintiff McCann and the New York Subclass)

390. Plaintiff realleges all previous paragraphs as if fully set forth below.

391. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law ("GBL") § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect the Plaintiff's and Class Members' Sensitive Information, which was a direct and proximate cause of the Data Breach, the Plaintiff's and Class Members' Sensitive Information being compromised, and subsequent harms caused to Plaintiff and Class Members;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures, despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach, the Plaintiff's and Class Members' Sensitive Information being compromised, and subsequent harms caused to the Plaintiff and Class Members;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Data Breach, Plaintiff's and Class Members' Sensitive Information being compromised, and subsequent harms caused to the Plaintiff and Class Members;

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

d. Misrepresenting that it would protect the privacy and confidentiality of the Plaintiff's and Class Members' Sensitive Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New York GBL § 349;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure the Plaintiff's and Class Members' Sensitive Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New York GBL § 349.

392. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Sensitive Information.

393. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and Class Members' rights. As mentioned above, prior data breaches in Defendant's industry put it on notice that its security and privacy protections were inadequate.

394. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

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

loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Sensitive Information; and an increased, imminent risk of fraud and identity theft.

395. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the numerous New York citizens affected by the Data Breach.

396. The deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid.

397. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

COUNT XI
Violation of the Illinois Private Information Protection Act
815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.
(On Behalf of Plaintiff Page and the Illinois Subclass)

398. Plaintiff realleges all previous paragraphs as if fully set forth below.

399. Defendant, as an entity that facilitates and/or takes responsibility for the collection, handling, dissemination, and other dealings with nonpublic Sensitive Information, qualifies as a Data Collector, as defined in 815 Ill. Comp. Stat. § 530/5.

400. Plaintiff's and Class Members' Sensitive Information (e.g., Social Security numbers) includes Sensitive Information as covered under 815 Ill. Comp. Stat. § 530/5.

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

401. As a Data Collector, Defendant is required to notify Plaintiff and Class Members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

402. The Data Breach described herein constituted a "breach of the [Defendant's] security system."

403. Because Defendant knew or reasonably believed that Plaintiff's and Class Members' Sensitive Information was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion.

404. As alleged above, Defendant unreasonably delayed informing Plaintiff and Class Members about the Data Breach, affecting their Sensitive Information, after Defendant knew that the Data Breach had occurred.

405. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Defendant violated 815 Ill. Comp. Stat. § 530/10(a).

406. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

407. As a result of Defendant's violation of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class Members because their stolen Sensitive Information would have had less value to identity thieves.

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

408. As a result of Defendant's violation of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

409. As a direct and proximate result of Defendant's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Class Members suffered damages as described herein.

410. Plaintiff and Class Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because Defendant's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

COUNT XII
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act 815 ILCS 505/1, *et seq*.
(On Behalf of Plaintiff Page and the Illinois Subclass)

411. Plaintiff realleges all previous paragraphs as if fully set forth below.

412. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

413. Plaintiff and Class Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

414. Defendant's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

415. Defendant's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Sensitive Information, which was a direct and proximate cause of the Data Breach;

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

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Sensitive Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

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

f. Failing to timely and adequately notify Plaintiff and Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that its cybersecurity measures did not reasonably or adequately secure Plaintiff's and Class Members' Sensitive Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

416. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability of Defendant to protect the confidentiality of consumers' Sensitive Information.

417. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

418. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

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

419. Defendant acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff's and Class Members' rights. Past data breaches within Defendant's industry put Defendant on notice that its cybersecurity measures were inadequate.

420. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive acts and practices, Plaintiff 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 loss of value of their Sensitive Information.

421. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT XIII
Violation of the Illinois Uniform Deceptive Trade Practices Act
815 ILCS 510/2, *et seq*.
(On Behalf of Plaintiff Page and the Illinois Subclass)

422. Plaintiff realleges all previous paragraphs as if fully set forth below.

423. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

424. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that it does not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

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

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

425. Defendant's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Sensitive Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Sensitive Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. §

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

45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Plaintiff and Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that its cybersecurity measures did not reasonably or adequately secure Plaintiff's and Class Members' Sensitive Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Sensitive Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

426. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability of Defendant to protect the confidentiality of consumers' Sensitive Information.

427. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Class

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

Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

428. As a result of Defendant's violations of the Illinois Uniform Deceptive Trade Practices Act, Plaintiff and Class Members suffered damages, as described above, and are likely to suffer harm in the future from the deceptive conduct absent injunctive relief.

429. As a proximate result of Defendant's acts and omissions, Plaintiff's and the Class Members' Sensitive Information were acquired by a third party and is now available for disclosure and redisclosure without authorization.

430. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to the fact that Defendant continues to possess their Sensitive Information, despite its inadequate cybersecurity system and policies. A judgment for monetary damages will not end Defendant's inability and/or refusal to adequately safeguard the Sensitive Information of Plaintiff and Class Members.

PRAYER FOR RELIEF

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

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

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

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

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

D. Enjoining Defendant from further deceptive practices and making untrue statements to Plaintiffs about the Data Breach and the stolen Sensitive Information;

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

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

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

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

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

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: July 7, 2025

Respectfully submitted,

TOUSLEY BRAIN STEPHENS PLLC

By: */s/ Cecily C. Jordan*
Cecily C. Jordan, WSBA #50061
By: */s/ Jason T. Dennett*
Jason T. Dennett, WSBA #30686
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
Telephone: (206) 682-5600
Facsimile: (206) 682-2992
jdennett@tousley.com
cjordan@tousley.com

COTCHETT, PITRE & McCARTHY, LLP

By: /s/ Thomas E. Loeser
Thomas E. Loeser, WSBA # 38701
By: /s/ Karin Swope
Karin B. Swope, WSBA # 24015
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Telephone: (206)-802-1272
Facsimile: (206)-299-4184

Interim Co-Lead Counsel for Plaintiffs and the Putative Class

STRAUSS BORRELLI PLLC

By: /s/ Samuel J. Strauss
Samuel J. Strauss, WSBA #46971
Raina Borrelli (Pro Hac Vice forthcoming)
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

CLARKSON LAW FIRM, P.C.

By: /s/ Yana Hart
Yana Hart, Esq. (Pro Hac Vice)
By: /s/ Bryan P. Thompson
Bryan P. Thompson, Esq. (Pro Hac Vice)
Ryan Clarkson, Esq. (Pro Hac Vice forthcoming)
22525 Pacific Coast Highway
Malibu, CA 90265
Telephone: (213) 788-4050
rclarkson@clarksonlawfirm.com
yhart@clarksonlawfirm.com
bthompson@clarksonlawfirm.com

SHUB JOHNS & HOLBROOK LLP

By: /s/ Jonathan Shub
Jonathan Shub (Pro Hac Vice)
By: /s/ JBenjamin F. Johns
Benjamin F. Johns (Pro Hac Vice)
By: /s/ Samantha E. Holbrook
Samantha E. Holbrook (Pro Hac Vice)
By: /s/ Andrea L. Bonner

Andrea L. Bonner (Pro Hac Vice)
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Telephone: (610) 477-8380
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com
abonner@shublawyers.com

TYCKO & ZAVAREEI LLP

Sabita Soneji (Pro Hac Vice forthcoming)
1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6808
Facsimile: (202) 973-0950
ssoneji@tzlegal.com

GEORGE FELDMAN MCDONALD, PLLC

By: */s/ Lori G. Feldman*
Lori G. Feldman, WSBA #29096
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Telephone: (917) 983-9321
lfeldman@4-justice.com
eservice@4-justice.com

CLAYEO C. ARNOLC
A PROFESSIONAL CORPORATION

By: */s/ M. Anderson Berry*
M. Anderson Berry, WSBA No. 63160
Gregory Haroutunian (Pro Hac Vice forthcoming)
Brandon P. Jack (Pro Hac Vice forthcoming)
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Plaintiffs' Steering Committee

EXHIBIT A

LABORATORY SERVICES COOPERATIVE

Date: April 10, 2025

Notice of Data Breach

Laboratory Services Cooperative (LSC) is encouraging individuals to take precautionary measures to protect their information following a security incident.

LSC provides lab testing services to select Planned Parenthood centers. If you, or someone whose healthcare bills you pay for, visited one of these centers and had lab tests done or were referred for lab tests, your information might be part of this incident.

Please be advised that this incident did not involve all Planned Parenthood centers. It specifically may have impacted only those centers that received lab testing services from LSC. It is important to note that LSC began providing services to these centers at different times, with some partnerships starting as recently as the past few years. For a list of states where LSC partners with Planned Parenthood centers, please see the FAQ section of this website notice.

We encourage individuals to read this notice carefully, as it contains important details about the incident and steps you can take to help protect your information.

What Happened?

On October 27, 2024, LSC identified suspicious activity within its network. In response, LSC immediately engaged third-party cybersecurity specialists to determine the nature and scope of the incident and notified federal law enforcement. The investigation revealed that an unauthorized third party gained access to portions of LSC's network and accessed/removed certain files belonging to LSC.

LSC promptly initiated a review and engaged a third-party vendor to help identify whose information may be potentially involved and to what extent.

What Information Was Involved?

In February 2025, LSC received the initial results of the data review, revealing that certain LSC patient and worker-related data might be affected.

The specific information involved is not the same for everyone. It depends on the individual's relationship with LSC but may include contact details such as name, address, phone number, and email, along with one or more of the following categories:

- Medical/Clinical Information: This may include information such as date(s) of service, diagnoses, treatment, medical record number, lab results, patient/accession number, provider name, treatment location, and related-care details.
- Health Insurance Information: This may encompass plan name, plan type, insurance companies, and member/group ID numbers.
- Billing, Claims, and Payment Data: This could involve claim numbers, billing details, bank account details (including bank name, account number, and routing number), billing codes, payment card details, balance details, and similar banking and financial information.
- Additional Identifiers: This may include Social Security Number, driver's license or state ID number, passport number, date of birth, demographic data, student ID number, and other forms of government identifiers.

For LSC workers, the information involved may also include details about their dependents or beneficiaries if that information was provided to LSC.

What We Are Doing.

Upon detecting the suspicious activity, we moved quickly to investigate the incident and secure our environment. We then conducted a thorough review to determine whose information may be potentially involved.

The confidentiality, privacy, and security of information maintained by LSC remains its top priority. As a precaution, LSC has hired third-party cybersecurity specialists to monitor the dark web for any information that may have been accessed or taken without authorization during this incident. The dark web is a hidden part of the internet where unauthorized activities and data exchanges often happen.

The cybersecurity specialists hired by LSC are using tools and techniques to scan various dark web forums, marketplaces, and other platforms. As of this writing, they haven't found any evidence that information involved in this incident is on the dark web.

LSC is offering free credit monitoring and medical identity protection services through CyEx Medical Shield Complete to individuals who suspect their information may be involved in this incident. A description of these services and enrollment instructions are provided in the next section.

What You Can Do.

We encourage individuals to review the steps outlined in this notice to protect their information. Cybersecurity is an ongoing concern for everyone, as companies worldwide face cybersecurity threats. By following the steps below, individuals can better protect themselves.

1. Enroll in Medical Shield Complete or Minor Defense

    a. CyEx Medical Shield Complete: LSC is offering free credit monitoring and medical identity protection services through CyEx Medical Shield Complete to individuals potentially affected by this incident. LSC is paying the cost for these services for 12 or 24 months, depending on state of residence. Please see below for key features and enrollment instructions.

    Key Features:

    - 1-Bureau Credit Monitoring
    - Health Insurance Plan Number Monitoring
    - Medical Record Number Monitoring
    - Medical Beneficiary Identifier Monitoring
    - National Provider Number Monitoring
    - International Classification of Diseases Monitoring
    - Health Savings Account Monitoring
    - Dark Web Monitoring

    How to Enroll:

    1. **Get Your Activation Code:** Call LSC's dedicated call center at 1-855-549-2662 (available Monday through Friday, 9:00 AM to 9:00 PM ET) to receive your unique Activation Code.

    2. **Visit the Enrollment Website:** For adults, go to: app.medicalshield.cyex.com/enrollment/activate/lscms. For minors, go to: app.minordefense.com/enrollment/activate/lscmd.

    3. **Enter Your Activation Code:** Input your unique Activation Code.

    4. **Redeem Your Code:** Click "Redeem Code."

    5. **Create Your Account:** Follow the prompts to set up your account.

    Deadline to Enroll: The deadline to enroll is July 14, 2025. After this date, the enrollment process will close, and your Medical Shield Complete code will no longer be active. Please enroll before the deadline to take advantage of these services.

Need Help? If you need assistance with the enrollment process or have questions, please call CyEx directly at 1-866-622-9303. Please remember, however, that you will need to obtain your unique Activation Code first by calling LSC's dedicated call center at 1-855-549-2662 (available Monday through Friday, 9:00 AM to 9:00 PM ET).

Important Information Relating to Enrollment and Minors: Medical Shield Complete may not be available for individuals who do not have established credit, a U.S. address (or one in its territories), or a valid Social Security number. For minors, LSC is offering a separate monitoring service called Minor Defense. To learn more about Minor Defense and how to enroll, please call LSC's dedicated call center at 1-855-549-2662 (available Monday through Friday, from 9:00 AM to 9:00 PM ET).

2. Review Your Accounts for Suspicious Activity. We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.

3. Order a Credit Report. If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. Contact information for the nationwide credit reporting agencies is provided in the next section.

4. Contact the Federal Trade Commission, Law Enforcement and Credit Bureaus. You may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.identitytheft.gov; call the FTC at 1-877-438-4338; or write to the FTC Consumer Response Center at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

   You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 740241 Atlanta, Georgia, 30374	P.O. Box 9701 Allen, TX 75013	P.O. Box 2000 Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-916-8800

5. Additional Rights Under the FCRA. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here.

   Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by: (i) visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf; or (ii) by writing to Consumer Financial Protection Bureau, 1700 G Street, NW, Washington, DC 20552.

6. Request Fraud Alerts and Security Freezes. You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

Equifax Fraud Alert	Experian Fraud Alert	TransUnion Fraud Alert
P.O. Box 105069 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ 1-800-525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 https://www.transunion.com/fraud-alerts 1-888-909-8872

In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ 1-888-298-0045	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze 1-888-397-3742	P.O. Box 160 Woodlyn, PA 19094 http://www.transunion.com/creditfreeze 1-888-916-8800

Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years
- Proof of current address, such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

7. **For Iowa Residents.** You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft at: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319; 1-515-281-5164; and www.iowaattorneygeneral.gov.

8. **For Maryland Residents.** You can obtain information about avoiding identity theft from the Maryland Attorney General at: Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023 (toll-free in Maryland) or 1-410-576-6300; www.marylandattorneygeneral.gov. LSC is located at 2001 E. Madison Street, Seattle, WA 98122 and can be contacted at 1-425-460-4522.

9. **For New York Residents.** You can obtain information about security breach response, identity theft prevention, and identity protection information from the New York State Office of the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755 (toll-free) or 1-800-788-9898 (TDD/TTY toll-free line); https://ag.ny.gov/; and the Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 1000; 1-212-416-8433; and https://ag.ny.gov/internet/resource-center.

10. **For North Carolina Residents.** You can obtain information about avoiding identity theft from the North Carolina Attorney General at: North Carolina Attorney General's Office 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 (toll-free in North Carolina) or 1-919-716-6400; and www.ncdoj.gov.

11. **For Residents of Oregon.** You may report suspected identity theft to law enforcement, including the Office of the Oregon Attorney General and the FTC. Contact information for the FTC is included in your notice. The Office of the Oregon Attorney General at: 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; and https://www.doj.state.or.us/.

12. **For Rhode Island Resident.** You can obtain information about avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit 150, South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. You have the right to obtain a police report, and to request a security freeze (charges may apply), as described above. Information pertaining to approximately 48 Rhode Island residents was potentially involved in this incident.

13. **For Washington, DC Residents.** You can obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, DC 20001; 1-202-727-3400; and www.oag.dc.gov. You have the right to request a security freeze (without any charge) as described above.

For More Information.

If you have concerns that are not addressed by this notice, LSC has established a dedicated toll-free call center for individuals to call should they have any additional questions or concerns. The call center can be reached at 1-855-549-2662 (available Monday through Friday from 9:00 AM to 9:00 PM ET).

We sincerely regret any concern this incident may cause and will continue to work hard to maintain the trust of our patients and partners.

Sincerely,

Laboratory Services Cooperative