UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

SEATTLE DIVISION

JANE DOE 1, individually and on behalf of all others similarly situated, Plaintiff, vs. LABORATORY SERVICES COOPERATIVE, Defendant.	Case No. **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Jane Doe 1, individually and on behalf of all others similarly situated, ("Plaintiff") brings this Action against Laboratory Services Cooperative ("Laboratory Services Cooperative" or "LSC" or "Defendant"). Plaintiff's allegations are based upon personal knowledge as to herself and her own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff's attorneys. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth, after a reasonable opportunity for discovery.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

INTRODUCTION

1. Laboratory Services Cooperative ("LSC") is a designated non-profit organization and independent clinical laboratory based in Seattle, Washington that offers diagnostic testing services to select Planned Parenthood health centers throughout the United States. Laboratory Services Cooperative was established in April 2010 as an independent non-profit organization, but originated as the Planned Parenthood of the Great Northwest ("PPGNW") Laboratory in Bremerton in May 2007.[1] Laboratory Services Cooperative is critical in supporting health centers that provide reproductive health services across more than 35 U.S. states, handling highly sensitive personal data, billing information, and lab testing results.[2]

2. To receive diagnostic testing services from certain Planned Parenthood clinics, patients are required to entrust Laboratory Services Cooperative with their highly sensitive and personally identifiable information ("PII") and personal health information ("PHI") (collectively "Private Information"), which Laboratory Services Cooperative uses to engage in its usual business activities as an affiliate of Planned Parenthood. To reassure its patients, Planned Parenthood promises patients that it and its affiliates, including Laboratory Services Cooperative, "respect and are committed to protecting the privacy of users of our websites, applications, and other online and electronic services"[3] and they "understand that health information about you and your healthcare is personal" and "are committed to protecting health information about you."[4] Laboratory Services Cooperative, however, failed to protect the patient information it was entrusted, compromising the

[1] Michael Romo, M.S PPGNW Bremerton Lab is Now the Laboratory Services Cooperative (LSC), FOCUS ON PLANNED PARENTHOOD, https://www.plannedparenthood.org/uploads/filer_public/27/3b/273b678d-184b-404e-841c-33af41ea1fcb/focus_spring_2010_web.pdf (last accessed).

[2] Richard Console, Jr., *Laboratory Services Cooperative Data Breach Impacts 1.6 Million Planned Parenthood Patients*, JDSUPRA, https://www.jdsupra.com/legalnews/laboratory-services-cooperative-data-9483682/ (last accessed April 17, 2025).

[3] *Privacy Policy*, PLANNED PARENTHOOD, https://www.plannedparenthood.org/planned-parenthood-california-central-coast/privacy-policy#fullpolicy (last accessed April 16, 2025April 17, 2025).

[4] *HIPAA Privacy Policy*, PLANNED PARENTHOOD, https://www.plannedparenthood.org/planned-parenthood-california-central-coast/hipaa (last accessed April 16, 2025).

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

personal information of over one million individuals (the "Data Breach"), as announced by Defendant on April 10, 2025.[5]

3. Laboratory Services Cooperative failed to properly secure and safeguard the highly valuable PII and PHI of its patients, including patients' full names, SSNs, driver's license or passport numbers, government-issued IDs, dates of service, diagnoses, treatments, lab results, health insurance information, billing details, bank and payment card information, and other personal information.[6] Laboratory Services Cooperative also failed to comply with industry standards to protect information systems that contain Private Information and failed to provide timely and adequate notice to Plaintiff and other members of the Class that their Private Information had been accessed and compromised.

4. As a result of Laboratory Services Cooperative's inadequate security and breach of its duties and obligations, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unauthorized criminal third party. Plaintiff and Class Members have suffered injuries as a direct and proximate result of Defendant's conduct. These injuries include: (i) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Private Information; (ii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) the continued, long term, and certain increased risk that unauthorized persons will access and abuse Plaintiff's and Class Members' Private Information; (iv) the continued and certain increased risk that the Private Information that remains in Defendant's possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake proper measures to protect the Private Information; (v) invasion of privacy and increased risk of fraud and identity theft; (vi) theft of their Private Information and the resulting loss of privacy rights in that information; (vii) diminution in value and/or lost value of Private Information, a form of

[5] *Laboratory Services Cooperative Security Incident*, LABORATORY SERVICES COOPERATIVE, https://www.lscincidentsupport.com/ (last accessed April 16, 2025).
[6] *Id.*

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

property that Defendant obtained from Plaintiff and Class Members. This action seeks to remedy these failings and their consequences. Plaintiff and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they should be entitled to injunctive and other equitable relief.

5. While the breach here was especially sensitive, even the most basic Private Information becomes especially valuable to cybercriminals to create seemingly legitimate, personalized phishing scams. This exfiltrated personal data, the full extent of which Laboratory Services Cooperative has failed to disclose to the public, allows hackers to gain a clear image of each individual and track their whereabouts, leading hackers to each victim's behavior and background. The combined exfiltrated data effectively provides criminals with a key to their personal lives, making it easy to match additional data, gaining access to their personal accounts and insight on their preferences. Hackers are now able to build a three-dimensional picture and thereby exploit Laboratory Services Cooperative's patients.

6. Laboratory Services Cooperative has disregarded the rights of Plaintiff and Class Members by, inter alia, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to properly train its staff and employees on proper security measures.

7. In addition, Laboratory Services Cooperative failed to properly monitor its computer network and systems that housed the Private Information. Had it properly monitored these electronic and cloud-based systems, it would have discovered the intrusion sooner or prevented it altogether.

8. Defendant has also been unjustly enriched, as Plaintiff and the Class Members paid for medical services from their provider with the reasonable belief that it would be kept confidential and secure, including by Defendant and any vendors or affiliates their medical providers used. Defendant should have invested a greater portion of the monies received from Plaintiff and Class

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

Members in proper data management and security, including proper and safe storage of Plaintiff's and Class Members' Private Information. Because Defendant failed to implement data management and security measures sufficient to protect that data and comply with industry standards, the principles of equity and justice demand that Defendant not be permitted to retain the money Plaintiff and Class Members paid Defendant for protection they did not receive.

9. Plaintiff brings this lawsuit on behalf of herself and all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained. To remedy these violations of law, Plaintiff and Class Members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

PARTIES

Plaintiff

10. **Jane Doe 1** [7]**:** Plaintiff Doe is a natural person and citizen of California. Plaintiff visited a Planned Parenthood location in Lakewood, California, in August 2024, where her medical provider performed tests that, upon information and belief, were processed by Defendant. Plaintiff only allowed her medical provider and, by extension, Defendant, to maintain, store, and use her Private Information because she reasonably expected that Defendant would use proper security measures to protect her Private Information and prevent its access by unauthorized third parties. As a result of this expectation, Plaintiff entrusted her Private Information to Defendant, and her Private Information was within the possession and control of Defendant at the time of the Data Breach. Had Plaintiff been informed of Defendant's insufficient data security measures to protect her Private Information, she would not have willingly provided her Private Information to Defendant.

[7] Given the significant privacy concerns at stake, Plaintiff respectfully requests permission to proceed pseudonymously and will file a Motion to Proceed Pseudonymously if necessary.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

11. In order to receive laboratory testing services from her medical provider, and, by extension, Laboratory Services Cooperative, Plaintiff was required to, and did, provide her Private Information to Planned Parenthood, who then provided it to Laboratory Services Cooperative, which input it into their systems as well.

12. Upon information and belief, Defendant has not provided actual notice to all individuals affected by the Data Breach.

13. As a result of the Data Breach, Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

14. When Plaintiff's Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

15. Given the highly sensitive nature of the information involved, the Data Breach has also caused Plaintiff to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her Private Information. This highly sensitive information is now in the hands of criminals as a direct and proximate result of Defendant's misconduct. It is also possible that other forms of information not yet disclosed by Defendant were also lost in the breach.

16. As a result of the actual harm Plaintiff has suffered and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including self-monitoring her accounts to ensure no fraudulent activity has occurred, dealing with a marked increase in spam texts and emails that occurred soon after the breach, and changing identifying information and passwords for her accounts. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

17. The substantial risk of imminent harm and loss of privacy has also caused Plaintiff to suffer stress, fear, emotional distress, and anxiety.

18. Defendant acknowledged the risk posed to Class Members and their Private Information as a result of the Data Breach, explicitly stating that Laboratory Services Cooperative "sincerely regret[s] any concern this incident may cause and will continue to work hard to maintain the trust of [its] patients and partners," encouraging patients to "remain vigilant by regularly reviewing [their] accounts and monitoring credit reports for suspicious activity."[8]

Defendant

19. **Laboratory Services Cooperative.** Defendant Laboratory Services Cooperative is a designated non-profit organization based in Seattle, Washington, with its principal place of business located at 2001 E Madison St, Seattle, WA 98122. Defendant conducts business, providing laboratory testing services to Planned Parenthood health centers and their patients across thirty-five (35) U.S. states.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332(d) because this is a class action where the aggregate amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.

21. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District: Defendant's principal place of business is located in this District from where its board of directors and/or officers direct Defendant's activities including to their actions and inactions leading to the data breach at issue; Defendant gains revenue and profits from doing business in this District; Class Members were affected by the breach from Laboratory Services Cooperative's

[8] *Laboratory Services Cooperative Security Incident*, LABORATORY SERVICES COOPERATIVE, https://www.lscincidentsupport.com/ (last accessed April 16, 2025April 17, 2025).

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

actions and inactions directed from this District.

FACTUAL ALLEGATIONS

22. Laboratory Services Cooperative is a provider of diagnostic laboratory testing services for numerous Planned Parenthood clinics. Defendant collects and processes the personal data of its affiliates' patients, including those patients of Planned Parenthood clinics across thirty-five (35) U.S. states. To purchase services from Defendant, patients are forced to entrust Defendant with their Private Information.

23. The information collected and stored by Defendant includes, but is not limited to, personal identifiers, such as ***full names, SSNs, driver's license or passport numbers***, medical information, such as ***dates of service, diagnoses, treatments, and lab results***, health insurance information, such as ***plan types, insurers, and member/group ID numbers***, and billing and financial information, such as ***claims, billing details, and bank/payment information***.

24. Defendant holds itself as a trustworthy entity, which recognizes and values its patients' privacy and personal information and has repeatedly assured its patients of this through its affiliation with Planned Parenthood.

25. Plaintiff and other similarly situated patients relied to their detriment on Defendant's uniform representations and omissions regarding data security, including Defendant's failure to alert patients that its security protections were inadequate, and that Defendant would forever store Plaintiff's and Class Members' Private Information, failing to archive it, protect it, or at the very minimum warn consumers of the anticipated and foreseeable data breach.

26. Plaintiff and other similarly situated patients trusted Defendant with their sensitive and valuable Private Information.

27. Had Defendant disclosed to Plaintiff and its other patients that its data systems were not secure and were vulnerable to attack, Plaintiff would not have purchased Defendant's services.

The Data Breach

28. At all material times, Laboratory Services Cooperative failed to maintain proper security measures despite its promises of safety and security to consumers.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

29. On October 27, 2024, Defendant's computer system was breached by cybercriminals due to Defendant's failure to properly secure its network.[9] Defendant did not notify its patients then, nor make any announcements to alert them of this major security issue. By February 2025, the investigation conducted by third-party digital forensics specialists revealed that personal information, including personal health information, relating to certain Laboratory Services Cooperative patients and employees, was acquired by the threat actors. Despite being informed of the cyberattack on October 27, 2024, Defendant kept silent and chose not to notify the affected patients for nearly six months—a surprising and inexcusable delay further underscoring Defendant's disregard for its patients.

30. On or around April 10, 2025, Defendant finally began notifying some patients, including Plaintiff, of the Data Breach via a website posting after nearly six months had passed since Defendant learned of the unauthorized access.

31. In its statement, Defendant fails to include sufficient information about the Data Breach and what it is doing to fix the vulnerabilities and keep patients' information secure, leaving many consumers to speculate whether it is likely that their PII/PHI has been compromised and whether it is still safe in Defendant's hands. Instead, Defendant downplayed the extent of the Data Breach, and the harm to affected victims.

Data Breaches and the Market for PII/PHI

32. It should be no surprise that in today's digital economy, "a new form of black gold has emerged, one that is intangible yet infinitely more powerful: data."[10] Personal data has become a "precious commodity," at the forefront of technological innovation.[11] Data is a pivotal economic asset and form of capital, allowing companies rich in it to drive competition. Considering the

[9] *Steve Alder, Laboratory Services Cooperative Breach Impacts 1.6 Million People*, THE HIPAA JOURNAL, https://www.hipaajournal.com/laboratory-services-cooperative-data-breach/ (last accessed April 16, 2025).
[10] Lawrence Teixeira, *The New Black Gold: How Data Became the Most Valuable Asset in Tech*, MEDIUM (Feb. 12, 2024), https://medium.com/@lawrenceteixeira/the-new-black-gold-how-data-became-the-most-valuable-asset-in-tech-9e4541262ddf#:~:text=Lawrence%20Teixeira%20%7C%20Medium-,The%20New%20Black%20Gold:%20How%20Data%20Became,Most%20Valuable%20Asset%20in%20Tech&text=In%20the%20annals%20of%20history,most%20valuable%20asset%20in%20technology.&text=If%20playback%20doesn%27t%20begin%20shortly%2C%20try%20restarting%20your%20device.
[11] *Id.*

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

implications of "big data" in corporate America and the consequences of cyber thefts, which include heavy prison sentences, the value of data is axiomatic. Even this obvious risk-to-reward analysis illustrates beyond doubt that personal information has considerable market value.

33. In a consumer-driven world, the ability to capture and use consumer data to shape products, solutions, and the buying experience is critically important to a business's success.[12] Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin"[13] and that "[d]ata-driven companies are 23 times more likely to top their competitors in customer acquisition, about 19 times more likely to stay profitable and nearly seven times more likely to retain customers."[14]

34. Indeed, an entire economy exists related to the value of personal data. In 2023, the big data technology market was valued at roughly $349 billion, and that value is expected to grow from roughly $397 billion in 2024 to $1,194 billion by 2032.[15]

35. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[16] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[17] The OECD indicated that "[a]t the time of writing, the following elements of personal data were

---

[12] Laci Loew, *Data Differentiation: Why Consumer Data Is A Modern Organization's Real Competitive Advantage*, FORBES (Oct. 2, 2024), https://www.forbes.com/councils/forbescommunicationscouncil/2024/10/02/data-differentiation-why-customer-data-is-a-modern-organizations-real-competitive-advantage/ (last accessed April 16, 2025April 17, 2025).

[13] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, MCKINSEY (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data (last accessed April 16, 2025).

[14] Laci Loew, *Data Differentiation: Why Consumer Data Is A Modern Organization's Real Competitive Advantage*, FORBES (October 2, 2024), https://www.forbes.com/councils/forbescommunicationscouncil/2024/10/02/data-differentiation-why-customer-data-is-a-modern-organizations-real-competitive-advantage/ (last accessed April 16, 2025April 17, 2025).

[15] *Big Data Technology Market Size, Share & Industry Analysis*, FORTUNE BUSINESS INSIGHTS (Jan. 2025), https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144 (last accessed April 16, 2025April 17, 2025).

[16] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf (last accessed April 16, 2025April 17, 2025).

[17] *Id.* at 25.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military [record] is estimated to cost USD 55."[18]

36. Consumer concerns for how companies use their data is on the rise. According to Pew Research, 81% of U.S. adults are concerned about how companies use the data they collect about them.[19] Consumers increasingly say they don't understand what companies are doing with their data, with 67% of U.S adults saying they understand little to nothing about what companies are doing with their personal data, up from 59% in 2019.[20]

37. When a victim's data is compromised in a breach, the victim is exposed to serious ramifications regardless of the sensitivity of the data, including but not limited to identity theft, fraud, decline in credit, inability to access healthcare, as well as legal consequences.[21]

38. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that resolution of those problems could take more than a year.[22] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

39. The U.S. Government Accountability Office ("GAO") has concluded that it is common for data thieves to hold onto stolen data for extended periods of time before utilizing it for

---

[18] *Id.*

[19] *How Americans View Data Privacy,* PEW RESEARCH CENTER (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/; *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[20] *Id.*

[21] *Data Breach Response: A Guide for Business*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed April 16, 2025).

[22] *Victims of Identity Theft*, U.S. DEPARTMENT OF JUSTICE, (Sept. 2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last accessed April 16, 2025).

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

identity theft.[23] In the same report, the GAO noted that while credit monitoring services can assist with detecting fraud, those services do not stop it.[24]

40. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and financial fraud.[25] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the "dark web."

41. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

42. With repeated warnings from FTC, GAO, Department of Justice, and FBI – Defendant's had duty to do more, not less – especially because it was in possession of highly sensitive medical data – the data that cannot be changed for Plaintiff and the Class. Defendant has no exclude for its failure to implement robust security measures and instead ignore the warnings, and the cybersecurity mandated by the industry standard.

43. When companies entrusted with personal data fail to implement industry's best practices, cyberattacks and other data exploitations can go undetected for a long period of time. This worsens the ramifications and can even render the harm irreparable.

44. In this black market, criminals seek to sell the spoils of their cyberattacks to identity thieves who desire the data to extort and harass victims and take over victims' identities to open financial accounts and otherwise engage in illegal financial transactions under the victims' names.

45. PII has a distinct, high value—which is why legitimate companies and criminals seek to obtain and sell it. The market for individuals' data continues to grow.[26]

---

[23] *Data Breaches – Range of Consumer Risks Highlights Limitations of Identity Theft Services*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, https://www.gao.gov/assets/700/697985.pdf (last accessed April 16, 2025).

[24] *Id.*

[25] *What To Know About Identity Theft*, FEDERAL TRADE COMMISSION, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed April 16, 2025April 17, 2025).

[26] Emily Wilson, *The Worrying Trend of Children's Data Being Sold on the Dark Web*, TNW (Feb. 23, 2019), https://thenextweb.com/news/children-data-sold-the-dark-web (last accessed April 16, 2025April 17, 2025).

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

46. Indeed, an entire economy exists related to the value of personal data. In 2023, the big data technology market was valued at roughly $349 billion, and that value is expected to grow from roughly $397 billion in 2024 to $1,194 billion by 2032.[27]

47. Defendant knew or should have known that Plaintiff's and Class Members' Private Information is valuable, both to legitimate entities, like Defendant, and to cybercriminals.

48. Defendant knew or should have known that Plaintiff and Class Members would reasonably rely upon and trust Defendant's promises regarding security and safety of their data and systems, and that their valuable Private Information would be protected.

49. By collecting, using, selling, monitoring, and trafficking Plaintiff's and other patients' Private Information, and failing to protect it by maintaining inadequate security systems, failing to properly archive the Private Information, allowing access of third parties, and failing to implement security measures, Defendant caused harm to Plaintiff and other Laboratory Services Cooperative patients.

Defendant's Duty to Safeguard Private Information

50. Defendant collects, receives, and accesses patients' extensive individually identifiable information. This Private Information includes identifiers, such as full names, SSNs, driver's license of passport numbers, medical information, such as dates of service, diagnoses, treatments, and lab results, health insurance information, such as plan types, insurers, and member/group ID numbers, and billing, and financial data, such as claims, billing details, and bank/payment information.

51. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that an entity's failure to maintain reasonable and appropriate data security for individuals' sensitive personal information is an

[27] *Big Data Technology Market Size, Share & Industry Analysis*, FORTUNE BUSINESS INSIGHTS (Jan. 2025), https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144 (last accessed April 16, 2025.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

"unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

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

53. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all decision-making.[28]

54. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[29] The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

55. The FTC further recommends that entities not maintain PII or PHI longer than needed for the 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.[30]

---

[28] *Start With Security*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed April 16, 2025).

[29] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed April 16, 2025April 17, 2025).

[30] *Start With Security*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed April 16, 2025April 17, 2025).

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

56. Furthermore, FTC requires that entities like Defendant conduct risk assessments, implement and periodically review access control, encrypt customer information, implement multi-factor authentication, dispose of customer information securely, maintain a log of authorized users' activity and keep an eye out of unauthorized access, train employees regarding security awareness, conduct audits, penetration testing, and system wide scans regularly to test for publicly known security vulnerabilities—all of which if properly implemented would have allowed Defendant to prevent this Data Breach.

57. Defendant failed to properly implement basic data security practices, allowing for this data breach to occur and victimizing thousands of people by failing to adhere to many of the FTC protocols and allowing access to a hacker who was able to exfiltrate substantial amounts of consumer data. Defendant should have a multifaceted security protocol in place, including a program that adequately trains employees on recognizing and thwarting phishing and social engineering attacks, monitoring out-of-network emails, segmenting the network, flagging suspicious domain addresses or content, utilized multifactor authentication before allowing access to highly sensitive information, mandating strict compliance with these protocols; mandating regular archiving of email data/removal of sensitive data from emails to servers; avoiding exchanging any sensitive data for patients over the emails, simulating social engineering attempts to ensure compliance, increasing spam filtering via email gateways, implementing strict policies regarding exchange of PII/PHI over emails, implementing and enforcing appropriate credential/key procedures including finger print recognition/physical key authentication; monitoring systems 24/7 for any suspicious activity, encrypting data over the email exchanges. Had Defendant maintained these and other proper protocols and regularly conducted audits to ensure its vulnerabilities and training, it would have prevented this Data Breach.

58. Plaintiff and Class Members provided their Private Information to Laboratory Services Cooperative with the reasonable expectation and mutual understanding that Laboratory Services Cooperative would comply with its obligations to keep such information confidential and secure from unauthorized access.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

59. Laboratory Services Cooperative's failure to provide adequate security measures to safeguard members' Private Information is especially egregious because it operates in a field which has recently been a frequent target of scammers attempting to gain access to confidential PII/PHI.

Impact of the Data Breach on Consumers

60. Plaintiff and the Class have suffered actual harm as a result of Defendant's conduct. Defendant failed to institute adequate security measures that led to a data breach. This breach allowed hackers to access the Private Information of Plaintiff and the Class. Now that the Private Information has been accessed and absconded with, it is available for criminal elements to sell or trade and will continue to be at risk for the indefinite future. In fact, the U.S. Government Accountability Office found that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[31]

61. Plaintiff and Class Members are now vulnerable to a full gamut of cybercrimes, loss in value of their property, and have been forced to take remedial action, as listed below:

Digital Phishing Scams

62. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that people lost approximately $18.7 million to such scams in 2023 alone.[32]

63. Defendant knew or should have known of the dangers of digital phishing scams. When Personal Information is employed in a social engineering scheme, criminals can gain unfettered access to individuals, or corporate databases, as the Data Breach itself evinces.

64. Defendant's patients are now more likely to become victims of digital phishing attacks because of the compromised information.

Loss of Time

[31] *See* U.S. GOV'T ACCOUNTABILITY OFF. REPORT TO CONGRESSIONAL REQUESTERS 29 2007. https://www.gao.gov/new.items/d07737.pdf (last accessed April 16, 2025).

[32] *Internet Crime Report*, FEDERAL BUREAU OF INVESTIGATION, (2023), https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf scams (last accessed April 16, 2025).

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

65. As a result of this breach, Plaintiff and impacted consumers will suffer unauthorized email solicitations and experience a significant increase in suspicious phishing scam activity via email, phone calls, and text messages following the breach. In addition, Plaintiff, as a result of the breach, has spent significant time and effort researching the breach, monitoring her accounts for fraudulent activity, and dealing with increased unsolicited emails and texts.

Threat of Identity Theft

66. As a direct and proximate result of Defendant's breach of confidence, and failure to protect Private Information, Plaintiff and the Class have also been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Private Information, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen Private Information, illegal sales of the compromised Private Information on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties, decreased credit scores, lost work time, and other injuries. Defendant, through its misconduct, has enabled numerous bad actors to sell and profit off of Private Information that belongs to Plaintiff.

Out of Pocket Costs

67. Plaintiff is now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these services to avoid further impact. Plaintiff anticipates spending out of pocket expenses to pay for these services.

Diminution in Value of a Valuable Property Right

68. Because personal data is valuable personal property, market exchanges now exist where internet users like Plaintiff and Class Members can sell or monetize their own personal data.

69. In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

to legitimate marketers or app developers.[33] For example, consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[34]

70. Accordingly, as a result of the Data Breach, Plaintiff lost the sale value of her Private Information and the opportunity to control how it is used. That a threat actor specifically targeted Defendant demonstrates just how valuable Plaintiff's Private Information can be to hackers and the significant value of Plaintiff's Private Information to cybercriminals.

Loss of Privacy and Dignitary Harm

71. A data breach represents a significant violation of privacy, extending far beyond the mere loss of data. When sensitive personal information is compromised, individuals face a cascade of potential harm that erodes their sense of security and control, as information that they thought would remain confidential and private has now been leaked to the outside world, and which they no longer exercise control over. This exposure can lead to a profound sense of vulnerability, as individuals grapple with the knowledge that their most personal details are now in the hands of unknown actors, free to circulate and be publicized now, or at any time in the future.

72. Information regarding an individual's health and medical choices, such as here, is one of the most personal and private types of information that exists. An individual's right to privacy regarding their body, their medical care, and their reproductive choices are some of the most sacrosanct and inviolable rights an individual can possess. Harm relating to an individual's loss of privacy and dignitary harm has also long been recognized by courts and in the common law.

73. When an individual loses this privacy and their personal health and medical information is made public, such as here through its acquisition by criminal third parties, this harm cannot be undone. Defendant's failure to safeguard this sensitive information has stripped Plaintiff and the Class Members of this essential control, exposing them to the potential for enduring emotional distress and the profound sense of vulnerability that accompanies the public exposure of

[33] *See*, *e.g.*, *The Personal Data Revolution*, DATACOUP, https://datacoup.com/.

[34] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed April 16, 2025).

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

deeply private matters.

74. This is a fundamental violation of an individual's control over their own personal narrative and image to which they provide the world. By stripping Plaintiff and the Class Members of their right to control this information about themselves, Defendant has done immense harm to their rights to privacy as well as their personal dignity and bodily sovereignty. As a result, while difficult to quantify, this harm is very real, long-lasting, and severe and has caused real damage to Plaintiff and the Class Members, both emotionally as well as through their permanent loss of security and fundamental right to privacy and bodily autonomy.

Summary of Actual Economic and Noneconomic Damages

75. In sum, Plaintiff and similarly situated individuals were injured as follows:

i. Theft of their Private Information and the resulting loss of privacy rights in that information;

ii. Improper disclosure of their Private Information and the accompanying loss of privacy and dignitary harm;

iii. Loss of value of their Private Information;

iv. The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

v. Defendant's retention of profits attributable to Plaintiff's and other patients' Private Information that Defendant failed to adequately protect;

vi. Economic and non-economic impacts that flow from the imminent, and ongoing threat of fraud and identity theft to which Plaintiff is now exposed;

vii. Ascertainable out-of-pocket expenses and the value of Plaintiff's time allocated to fixing or mitigating the effects of this data breach;

viii. Overpayments for Defendant's services;

ix. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this data breach.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

Defendant Should Have Invested in Appropriate & Necessary Data Security

76. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks.

77. The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendant on notice, long before the Data Breach, that (1) cybercriminals were targeting companies who store personal health information, such as Defendant; (2) cybercriminals were ferociously aggressive in their pursuit of large collections of Private Information like that in possession of Defendant; (3) cybercriminals were selling large volumes of Private Information and corporate information on Dark Web portals; and (4) the threats were increasing.

78. Had Defendant been diligent and responsible, it would have implemented the basic cyber security steps necessary to protect the Private Information in its possession, by addressing the key vulnerabilities:

- Lack of a complete risk assessment, including internal, third-party, and cloud-based systems and services;
- Not promptly patching known/public vulnerabilities, and not having a way to process vulnerability reports;
- Misconfigured devices/servers;
- Unencrypted data and/or poor encryption key management and safeguarding;
- Use of end-of-life (and thereby unsupported) devices, operating systems, and applications;
- Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;
- Failure to block malicious email; and
- Users succumbing to business email compromise (BEC) and social exploits.[35]

[35] Gretel Egan, *OTA Report Indicates 93% of Security Breaches Are Preventable*, PROOFPOINT (Feb. 7, 2018), https://www.proofpoint.com/us/security-awareness/post/ota-report-indicates-93-security-breaches-are-preventable (last accessed April 16, 2025April 17, 2025).

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

79. Considering the information and warnings readily available to Defendant before the Data Breach, Defendant had reason to be on guard and to increase data security to avoid an attack.

80. Prior to the Data Breach, Defendant thus knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' Private Information could be accessed, exfiltrated, and utilized by nefarious individuals as the result of a cyberattack.

81. Data security experts advise that "the vast majority of data breaches are preventable" if companies follow widely-available advice on data security practices, including "continually audit[ing] and reevaluat[ing]" their data security practices; being aware of and working proactively to counter cybercriminals' evolving techniques and approaches; and training and re-training their employees.[36] Had Defendant maintained proper data security practices, this data breach too could have been prevented.

CLASS ALLEGATIONS

82. Plaintiff brings this action on her own behalf and on behalf of all other persons similarly situated. The Class which Plaintiff seeks to represent comprises:

> **Nationwide Class:**
> All individuals whose Private Information was exposed while in the possession of Defendant, or any of its subsidiaries and/or agents, during the Data Breach.
>
> **California Subclass:**
> All individuals who were citizens or residents of California when doing business with Defendant, whose Private Information was exposed while in the possession of Defendant, or any of their subsidiaries and/or agents, during the Data Breach.

This definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

83. The Class is comprised of approximately 1,600,000 of Laboratory Services Cooperative's patients who provided their Private Information, to Defendant, directly or indirectly,

[36] Nate Nead, *How To Prevent A Data Breach In Your Company*, FORBES (Jul. 30, 2021), https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=3828f7b918da (last accessed April 16, 2025April 17, 2025).

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

in order to obtain medical services in the past and were part of the Data Breach (the "Class Members"). The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

84. There is a well-defined community of interest in the questions of law and fact involved affecting the parties to be represented in that the Class was exposed to the same common and uniform false and misleading advertising and omissions. The questions of law and fact common to the Class predominate over questions which may affect individual Class members. Common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant's conduct is an unlawful business act or practice within the meaning of California Business and Professions Code § 17200, *et seq*., the Unfair Competition Law (UCL), which prohibits unfair, unlawful, or fraudulent business practices that harm consumers and competitors;

b. Whether Defendant's conduct is in violation of California Civil Code § 56, *et seq.*, the Confidentiality of Medical Information Act (CMIA);

c. Whether Defendant's conduct is in violation of California Civil Code §§1709 and 1710;

d. Whether Defendant's failure to implement effective security measures to protect Plaintiff's and the Class's Private Information was negligent;

e. Whether Defendant breached express and implied warranties of security to the Class;

f. Whether Defendant represented to Plaintiff and the Class that it would protect Plaintiff's and the Class Members' Private Information;

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

h. Whether Defendant breached a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

i. Whether Class Members' Private Information was accessed, compromised, or stolen in the Data Breach;

j. Whether Defendant's conduct caused or resulted in damages to Plaintiff and the Class;

k. Whether Defendant failed to notify the public of the breach in a timely and adequate manner;

l. Whether Defendant knew or should have known that its systems, including but not limited to training protocols and policies, left it vulnerable to the Data Breach;

m. Whether Defendant adequately addressed the vulnerabilities that allowed for the Data Breach; and

n. Whether, as a result of Defendant's conduct, Plaintiff and the Class are entitled to damages and relief.

85. Plaintiff's claims are typical of the claims of the proposed Class, as Plaintiff and Class Members were harmed by Defendant's uniform unlawful conduct.

86. Plaintiff will fairly and adequately represent and protect the interests of the proposed Class. Plaintiff has retained competent and experienced counsel in class action litigation and other complex litigation.

87. Plaintiff and the Class have suffered injury because of Defendant's false, deceptive, and misleading representations.

88. Plaintiff would not have allowed Defendant to have access to her Private Information but for the reasonable belief that Defendant would safeguard her data and Private Information.

89. The Class is identifiable and readily ascertainable. Notice can be provided to such patients using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

90. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually.

91. The litigation and resolution of the Class's claims are manageable. Individual litigation of the legal and factual issues raised by Defendant's conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

92. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class Members would create the risk of inconsistent or varying adjudications with respect to individual member of the Class that would establish incompatible standards of conduct for Defendant.

93. Absent a class action, Defendant will likely retain the benefits of its wrongdoing. Because of the small size of the individual Class Members' claims, few, if any, Class Members could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, Class Members will continue to suffer losses and Defendant (and similarly situated companies) will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains.

COUNT ONE

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW

BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.*

(*On Behalf of the California Subclass*)

94. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

///

///

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

A. "Unfair" Prong

95. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200, et seq., a challenged activity is "unfair" when "any injury it causes outweighs any benefits provide to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

96. Defendant's conduct as alleged herein does not confer any benefit to consumers. Mishandling this data shows blatant disregard for its patients' privacy and security.

97. Defendant's conduct as alleged herein causes injuries to consumers who do not receive services consistent with their reasonable expectations. Specifically, Defendant's patients would not have reason to believe that simply doing business with Defendant would place their Private Information in the hands of cybercriminals.

98. Defendant's conduct as alleged herein causes injuries to its patients, who entrusted Defendant with their Private Information and whose Private Information was leaked as a result of Defendant's unlawful conduct.

99. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in law, including the FTC Act, 15 U.S.C. §45, Cal. Civ. Code §1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

100. Defendant's patients cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

101. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

102. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of California Business and Professions Code Section 17200.

103. Defendant could have furthered its legitimate business interests in ways other than its unfair conduct.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

104. Defendant's conduct threatens members by failing to protect Plaintiff and the Class Members' Private Information from being exposed to hackers. Defendant's conduct also threatens other entities, large and small, who play by the rules. Defendant's conduct stifles competition, has a negative impact on the marketplace, and reduces consumer choice.

105. All the conduct alleged herein occurs and continues to occur in Defendant's operations. Defendant's wrongful conduct is part of a pattern or generalized course of conduct repeated consistently.

106. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

107. Plaintiff and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiff accordingly provided her Private Information to Defendant reasonably believing and expecting that her Private Information would be safe and secure. Plaintiff paid an unwarranted premium for the services she received.

108. Plaintiff and the Class would not have given Defendant their Private Information had they known that their Private Information was vulnerable to a data breach. Plaintiff and Class Members seek an order mandating that Defendant implement adequate security practices to protect patients' Private Information. Additionally, Plaintiff and Class Members seek an order awarding Plaintiff and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

B. "Fraudulent" Prong

109. California Business and Professions Code Section 17200, *et seq*. considers conduct fraudulent and prohibits said conduct if it is likely to deceive members of the public. *Bank of the West v. Superior Court*, 2 Cal. 4th 1254, 1267 (1992).

110. Defendant's implicit representations that it adequately protects consumer information are likely to deceive members of the public into believing that Defendant can be entrusted with

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

Private Information, and that Private Information gathered by Defendant is not in danger of being compromised.

111. Defendant's implied representations about its commitments to data security, as alleged in the preceding paragraphs, are false, deceptive, misleading, and unreasonable and constitute fraudulent conduct.

112. Defendant knew or should have known of its fraudulent conduct.

113. As alleged in the preceding paragraphs, the material misrepresentations by Defendant detailed above constitute a fraudulent business practice in violation of California Business & Professions Code Section 17200.

114. Defendant could have implemented robust security measures to prevent the Data Breach but failed to do so.

115. Defendant's wrongful conduct is part of a pattern or generalized course of conduct.

116. Pursuant to Business & Professions Code Section 17203, Plaintiff and the Class seek an order from this Court enjoining Defendant from continuing to engage, use, or employ its practice of false and deceptive representations about the strength or adequacy of its security systems. Likewise, Plaintiff and the Class seek an order requiring Defendant to disclose such misrepresentations.

117. Plaintiff and the Class have suffered injury in fact and have lost money as a result of Defendant's fraudulent conduct. Plaintiff paid an unwarranted premium for the services she received. Specifically, Plaintiff believed that her information would be secure with Defendant when she did business with them, when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to the Data Breach.

118. **Injunction**. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seek an order of this Court compelling Defendant to implement adequate safeguards to protect consumer Private Information retained by Defendant. This includes, but is not limited to improving security systems, deleting data that no longer needs to be retained by Defendant, archiving that data on secure servers, adopting adequate and robust training policies and protocols

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

for all employees entrusted with access to Personal Information and notifying all affected consumers in a timely manner.

C. "Unlawful" Prong

119. California Business and Professions Code Section 17200, *et seq*., identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.,* 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

120. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates California Civil Code Section 1750, *et seq.*

121. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

122. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California common law.

123. Defendant knew or should have known of its unlawful conduct.

124. As alleged in the preceding paragraphs, the misrepresentations and failure to disclose the lack of data security by Defendant detailed above constitute an unlawful business practice within the meaning of California Business and Professions Code section 17200.

125. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

126. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

127. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

128. Plaintiff and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiff and the Class would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiff and Class Members seek an order mandating that Defendant implement adequate security practices to protect members' Private Information. Additionally, Plaintiff and the Class Members seek and request an order awarding Plaintiff and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

129. No adequate remedy at law. Plaintiff and the Class are entitled to equitable relief as no adequate remedy at law exists.

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

131. 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;

132. The equitable relief under the UCL (and also under unjust enrichment discussed below) creates a straightforward cause of action for violations of law (such as statutory or regulatory requirements related to representations and omissions made with respect to Defendant's services). Furthermore, damages for non-UCL claims require additional elements or pre-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.

133. 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

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

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.

COUNT TWO

VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CALIFORNIA CIVIL CODE SECTION 56, *et seq.*

(*On Behalf of the California Subclass*)

134. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

135. Defendant is subject to the requirements and mandates of the CMIA because it is a "contractor" and/or "provider of health care" pursuant to Cal. Civ. Code § 56.06.

136. CMIA section 56.36 allows an individual to bring an action against a "person or entity who has negligently released confidential information or records concerning him or her in violation of this part."

137. As a direct result of its negligent failure to adequately protect the data it collected from the Plaintiff and Class Members, Defendant allowed for a Data Breach which released the PII and PHI of Plaintiff and the Class Members to criminals and/or third parties.

138. The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care ... regarding a patient's medical history, mental or physical condition, or treatment."

139. The CMIA defines individually identifiable information as "medical information [that] includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patients name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." Cal. Civ. Code § 56.050.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

140. Defendant is in possession of affected individuals' medical information, as it has indicated that its patients' medical and clinical information, including diagnoses, treatment information, medical record numbers, and more, was lost in the data breach. Thus, information relating to the diagnosis and treatment of patients, at minimum, was exposed in the data breach. Further, the compromised data was individually identifiable because it was accompanied by elements sufficient to allow identification of Plaintiff by the third parties to whom the data was disclosed. Class Members' PII was included in the Data Breach.

141. Defendant came into possession of Plaintiff's and Class Members' medical information and had a duty pursuant to Section 56.06 and 56.101 of the CMIA to maintain, store and dispose of the Plaintiff's and Class Members' medical records in a manner that preserved their confidentiality. Sections 56.06 and 56.101 of the CMIA prohibit the negligent creation, maintenance, preservation, store, abandonment, destruction, or disposal of confidential medical information.

142. Defendant further violated the CMIA by failing to use reasonable care, and, in fact, negligently maintained Plaintiff's and Class Members' medical information, allowing and enabling a threat actor to view and access unencrypted PHI for Class Members.

143. As a direct and proximate result of Defendant's violations of the CMIA, Plaintiff and Class Members have been injured and are entitled to compensatory damages, punitive damages, and nominal damages of one-thousand dollars ($1,000) for each of Defendant's violations of the CMIA, as well as attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

COUNT THREE

DECEIT BY CONCEALMENT, CALIFORNIA CIVIL CODE SECTIONS 1709, 1710

(*On Behalf of the California Subclass*)

144. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

145. Defendant knew or should have known that its internal systems were inadequate to protect Class Members' Private Information. Specifically, Defendant had an obligation to disclose

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

to its patients that its internal systems were not adequate to safeguard their Private Information. Defendant did not do so. Rather, Defendant deceived Plaintiff and the Class by concealing the vulnerabilities in its systems.

146. Even after Defendant discovered the Data Breach had impacted sensitive Private Information, it concealed it, and waited nearly six months before announcing it to the public so consumers could know and take precautions against the Data Breach.

147. California Civil Code §1710 defines deceit as, (a) "[t]he suggestion, as a fact, of that which is not true, by one who does not believe it to be true"; (b) "[t]he assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true"; (c) "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact"; or (d) "[a] promise, made without any intention of performing it." Defendant's conduct as described herein therefore constitutes deceit of Plaintiff and the Class.

148. California Civil Code §1709 mandates that in willfully deceiving Plaintiff and the Class with intent to induce or alter their position to their injury or risk, Defendant is liable for any damages which Plaintiff and the Class thereby suffer.

149. As described above, Plaintiff and the Class have suffered significant harm as a direct and proximate result of Defendant's deceit and other unlawful conduct. Had Defendant been truthful about its security vulnerabilities or had promptly and adequately notified affected parties that their information had been compromised, Plaintiff and the Class would not have suffered some, if not all, of the harms attributable to the Data Breach. Specifically, Plaintiff and the Class have been subject to numerous attacks, including an increase in spam texts and other scam attempts. Defendant is liable for these damages as well.

///

///

///

///

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

COUNT FOUR

NEGLIGENCE

(*On Behalf of the Nationwide Class*)

150. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

151. Defendant owed a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that consumers' Private Information was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

152. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiff and Class Members, who were the foreseeable and probable victims of any inadequate security practices.

153. Defendant had a special relationship with Plaintiff and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach. Plaintiff and Class Members were compelled to entrust Defendant with their Private Information. At relevant times, Plaintiff and Class members understood that Defendant would take adequate security precautions to safeguard that information. Only Defendant had the ability to protect Plaintiff's and Class Members' Private Information it held.

154. Defendant knew or should have known that Plaintiff's and the Class Members' Private Information is information that is frequently sought after by criminals.

155. Defendant knew or should have known that Plaintiff and the Class members would suffer harm if their Private Information was leaked.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

156. Defendant knew or should have known that its security systems were not adequate to protect Plaintiff's and the Class Members' Private Information from a data breach.

157. Defendant knew or should have known that adequate and prompt notice of the Data Breach was required such that Plaintiff and the Class could have taken more swift and effective action to change or otherwise protect their Private Information. Defendant failed to provide timely notice upon discovery of the data breach. Class Members were informed of the data breach on April 10, 2025, with many not receiving actual notice. Defendant had learned of the data breach nearly six months prior, in October 2024.

158. Defendant's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiff's and the Class Members' Private Information by failing to design, implement, and maintain adequate security measures to protect this information. Moreover, Defendant did not implement, design, or maintain adequate measures to detect a data breach when it occurred.

159. Defendant's conduct as described above constituted an unlawful breach of its duty to provide adequate and prompt notice of the data breach.

160. Plaintiff's and the Class Members' Private Information would have remained private and secure had it not been for Defendant's wrongful and negligent breach of its duties. The leak of Plaintiff's and the Class Members' Private Information, and all subsequent damages, was a direct and proximate result of Defendant's negligence.

161. Defendant's negligence was, at least, a substantial factor in causing Plaintiff's and the Class's Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing Class Members' other injuries arising out of the Data Breach.

162. The damages suffered by Plaintiff and the Class were the direct and reasonably foreseeable result of Defendant's negligent breach of its duties to adequately design, implement, and maintain security systems to protect Plaintiff's and Class Members' Private Information.

163. Defendant knew or should have known that its security for safeguarding Plaintiff's and Class Members' Private Information was inadequate and vulnerable to a data breach.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

164. Defendant's negligence directly caused significant harm to Plaintiff and Members of the Class.

COUNT FIVE

BREACH OF EXPRESS WARRANTY

(*On Behalf of the Nationwide Class*)

165. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

166. Defendant made an express warranty to Plaintiff and Class Members that it is committed to protecting the Private Information entrusted to it, by representing the same to Plaintiff's and the Class Members' medical providers. In order to obtain Defendant's services, Plaintiff and Class Members were required to provide their Private Information which they reasonably believed, based on their medical providers express representations, would be kept private and secure.

167. Defendant's express warranties regarding its security standards made to Plaintiff and the Class appear throughout Planned Parenthood's Privacy Policy, which explicitly applies not only to Planned Parenthood itself but also to its affiliates, including Laboratory Services Cooperative.[37] The promise of security is associated with the offerings and services, and therefore becomes the basis of the bargain.

168. Plaintiff and the Class engaged in business with Defendant, including entrusting it with their Private Information, with the expectation that the information they provided would be kept safe, secure, and private in accordance with the express warranties made by Defendant through Planned Parenthood's website and Privacy Policy.

169. Defendant breached the express warranties made to Plaintiff and Class Members by failing to provide adequate security to safeguard Plaintiff's and the Class's Private Information. As

[37] *Privacy Policy*, PLANNED PARENTHOOD, https://www.plannedparenthood.org/planned-parenthood-california-central-coast/privacy-policy#fullpolicy (last accessed April 16, 2025April 17, 2025).

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

a result, Plaintiff and Class Members suffered injury and deserve to be compensated for the damages they suffered.

170. Plaintiff and Class Members paid money to purchase services from Defendant. However, Plaintiff and Class Members did not obtain the full value of the advertised services. If Plaintiff and other Class Members had known that their Private Information would be exposed as a result of their purchasing the services, then they would not have purchased the services.

171. Plaintiff and the Class are therefore entitled to recover all available remedies for said breach of express warranty, as this Court deems proper.

COUNT SIX

BREACH OF IMPLIED CONTRACT

(*On Behalf of the Nationwide Class*)

172. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

173. At all relevant times, Defendant had a duty, or undertook and/or assumed a duty, to implement a reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and notification procedures, in order to safeguard the Private Information of Plaintiff and the Class Members, and to prevent the unauthorized access to and disclosures of this data.

174. Among other things, Plaintiff and Class Members were required to disclose their Private Information to Defendant when doing business with it, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

175. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

176. By entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

177. Under implied contracts, Defendant and/or their affiliated providers promised and were obligated to protect Plaintiff's and Class Members' Private Information. In exchange, Plaintiff and Members of the Class agreed to turn over their Private Information.

178. Defendant's express representations, including, but not limited to the express representations found in their notices of privacy practices, memorialize and embody the implied contractual obligations requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

179. Plaintiff and Class Members performed their obligations under the contract when they provided their Private Information in consideration for Defendant's services.

180. Defendant materially breached its contractual obligations to protect the Private Information it gathered when the information was accessed and exfiltrated during the Data Breach.

181. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant notices of privacy practices. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its notification of the Data Breach to Plaintiff and Class Members.

182. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

183. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive full benefit of the bargain they entered into.

184. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiff, Class Members, nor any reasonable person would have entered into the aforementioned contracts with Defendant.

185. As a direct and proximate result of the data breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

COUNT SEVEN

BREACH OF CONFIDENCE

(*On Behalf of the Nationwide Class*)

186. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

187. Plaintiff and Class Members maintained a confidential relationship with Defendant whereby Defendant undertook a duty not to disclose to unauthorized parties the Plaintiff's and Class Members' Private Information to unauthorized third parties. Such Private Information was confidential and novel, highly personal and sensitive, and not generally known.

188. Defendant knew Plaintiff's and Class Members' Private Information was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the Private Information it collected, stored, and maintained.

189. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class Members' Private Information in violation of this understanding. The unauthorized disclosure occurred because Defendant failed to implement and maintain reasonable safeguards to protect the Private Information in its possession and failed to comply with industry-standard data security practices.

190. Plaintiff and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

191. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, or used by unauthorized third parties.

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

192. Defendant knew its computer systems and technologies for accepting, securing, and storing Plaintiff's and Class Members' Private Information had serious security vulnerabilities because it failed to observe standard security practices or correct known security vulnerabilities.

193. The Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information, as well as the resulting damages.

194. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information.

195. As a direct and proximate result of Defendant's violations, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT EIGHT

INVASION OF PRIVACY

(*On Behalf of the Nationwide Class*)

196. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

197. Plaintiff and Class Members had a reasonable and legitimate expectation of privacy in their Private Information that Defendant failed to adequately protect against compromise from unauthorized third parties.

198. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

199. Defendant failed to protect, and released to unknown and unauthorized third parties, the Private Information of Plaintiff and Class Members.

200. By failing to keep Plaintiff's and Class Members' Private Information safe, knowingly utilizing unsecure systems and practices, Defendant unlawfully invaded Plaintiff's and Class Members' privacy by, among others, (i) intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

secure their Private Information from disclosure to unauthorized persons and/or third parties; and (iii) enabling the disclosure of Plaintiff's and Class Members' Private Information without consent.

201. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class Members' position would consider its actions highly offensive.

202. Defendant knew, or acted with reckless disregard of the fact that, organizations handling PII or PHI are highly vulnerable to cyberattacks and that employing inadequate security and training practices would render them especially vulnerable to data breaches.

203. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted, thereby causing Plaintiff and the Class Members undue harm.

204. Plaintiff seeks injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiff and Class Members. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT NINE

UNJUST ENRICHMENT

(*On Behalf of the Nationwide Class*)

205. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

206. Defendant funds its data security measures entirely from its general revenues, including payments made by or on behalf of Plaintiff and Class Members.

207. A portion of the payments made by or on behalf of Plaintiff and Class Members was to be used to provide the necessary level of data security.

208. Plaintiff and the Class conferred a monetary benefit on Defendant by obtaining tests from their medical provider, which in turn contracted with Defendant to perform the testing. In

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

doing so, Plaintiff and Class Members provided Defendant with their most sensitive PII and PHI. In exchange, Plaintiff and Class Members should have received from Defendant the services that were subject to the transaction and had their PII protected with adequate data security measures.

209. Defendant knew that Plaintiff and the Class conferred a benefit which it accepted, and through which Defendant was unjustly enriched. Defendant profited from these transactions and used Plaintiff's and the Class's PII and PHI for business purposes to increase their revenues.

210. Defendant enriched itself by saving the costs it reasonably should have spent on the necessary data security measures to secure Plaintiff's and the Class Members' PII and PHI. Instead of providing the necessary level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and the Class, by using ineffective security measures, failing to pay money for the much-needed training of its employees, failing to conduct the audits, implementing other security measures discussed above. Plaintiff and the Class suffered an injury as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and training.

211. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and the Class, because it failed to implement appropriate data management and security measures as mandated by common law and statutory duties.

212. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information nor would they have done business with Defendant.

213. Plaintiff and the Class have no adequate remedy at law as discussed above.

214. Defendant should be compelled to disgorge its profits and/or proceeds that it unjustly received as a result of having Plaintiff's and Class Members' Private Information, or alternatively, Defendant should be compelled to refund the amounts that Plaintiff and the Class overpaid for its services.

///

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

COUNT TEN

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT

(*On Behalf of the Nationwide Class*)

215. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

216. Defendant entered into a contract with each medical service provider to provide laboratory testing services. These contracts were made expressly for the benefit of the Plaintiff and Class Members, who gave their Private Information to their Medical Provider directly, as well as indirectly to the Defendant. Plaintiff and the Class Members only provided this information to their medical provider because they reasonably believed that their Private Information would be kept secure and private. In order to effectuate offered services, Defendant agreed to protect Plaintiff and Class Members' PII.

217. Thus, the benefit of collection, protection, and storage of the Private Information was the direct, intended, and primary objective of the contracting parties as it related to those express terms.

218. Defendant breached its contract with each medical provider when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff and Class Members' PII.

219. Defendant knew that if it breached its contract, the harm would befall the medical provider's stakeholders for whom the benefit was intended to confer, including the Plaintiff and the Class Members. As such, Defendant's failure to uphold the terms of its contract and allow for the Data Breach has foreseeably harmed Plaintiff and the Class Members.

220. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, along with their costs, including attorneys' fees incurred.

///

///

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

COUNT ELEVEN

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS AND INTRUSION UPON SECLUSION

(*On Behalf of the Nationwide Class*)

221. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

222. Plaintiff's and Class Members' Private Information is and always has been private and confidential.

223. Dissemination of Plaintiff's and Class Members' Private Information is not of a legitimate public concern; publication to third parties of their Private Information would be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable people.

224. By failing to keep Plaintiff's and Class Members' Private Information secure and disclosing Private Information to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion.

225. Defendant's wrongful actions and/or inaction constituted, and continue to constitute, an invasion of Plaintiff's and Class Members' privacy by publicly disclosing their Private Information.

226. Defendant's intrusions were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

227. Plaintiff and the Class Members were, and continue to be, damaged as a direct and proximate result of Defendant's invasion of their privacy by publicly disclosing their Private Information, for which they suffered loss and are entitled to compensation.

228. As a direct and proximate result of Defendant's violations, Plaintiff and the Class have suffered and continue to suffer injury.

///

///

///

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

COUNT TWELVE

DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF

(*On Behalf of the Nationwide Class*)

229. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

230. 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.

231. 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.

232. Defendant owes a duty of care to Plaintiff and Class Members which require it to adequately secure its Private Information when it chose to accept and store Plaintiff's and Class Members' Private Information.

233. Defendant still possesses Plaintiff's and Class Members' Private Information.

234. 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.

235. Plaintiff and Class Members are at risk of harm due to the exposure of their Private Information and the Defendant's failures to address the security failings that lead to such exposure.

236. 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 Plaintiff's and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their Private Information.

237. Plaintiff 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

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

consumers' Private 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' Private Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

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

d. Requiring Defendant to protect all data collected through any account creation requirements;

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

f. Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private 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;

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

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

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 Private Information data; and

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

238. 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 Plaintiff's and Class Members' Private Information.

239. If an injunction is not issued, Plaintiff 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.

240. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs, the Plaintiff and the Class will likely be subjected to fraud, identity theft, and other harms described herein. However, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is minimal given it has preexisting legal obligations to employ these measures.

///

///

///

///

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for judgment and relief on all cause of action as follows:

A. That the Court determines that this Action may be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order declaring that Defendant's actions, as set forth in this Complaint, violate the laws set forth above;

C. That the Court enter an order providing declaratory and injunctive relief including specific steps, as outlined above, requiring Defendant to utilize appropriate methods and policies as necessary to remediate the harm suffered by Plaintiff and the Class members as well as to prevent future harm and properly secure its data;

D. That the Court award Plaintiff and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

F. That the Court award Plaintiff and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

G. That the Court award Plaintiff and the Class their reasonable attorneys' fees and costs of suit;

COTCHETT, PITRE & McCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272

H. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and

I. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully demands a trial by jury for all claims so triable.

Dated: April 17, 2025

COTCHETT, PITRE & McCARTHY, LLP

/s/ Thomas E. Loeser
Thomas E. Loeser (SBN: 38701)
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272
Fax: (650) 697-0577
Email: *tloeser@cpmlegal.com*

CLARKSON LAW FIRM, P.C.
Ryan Clarkson, Esq. (*PHV forthcoming*)
Yana Hart, Esq. (*PHV forthcoming)*
Bryan P. Thompson, Esq. (*PHV forthcoming)*
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Email: *rclarkson@clarksonlawfirm.com*
Email: *yhart@clarksonlawfirm.com*
Email: *bthompson@clarksonlawfirm.com*