UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ROSE CLARKSON, JUNE MACK, VALERIE HICKS, CARRIE DEVERS, THERESA CULVER, AMY CAPODICI, GEORGEANN ROBERTS, and PAMELA SILVER, on behalf of themselves and all others similarly situated, Plaintiffs, v. ONSITE MAMMOGRAPHY, LLC, d/b/a ONSITE WOMEN'S HEALTH, Defendant.	Civil Action No. 3:25-cv-11123-MGM **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Rose Clarkson, June Mack, Valerie Hicks, Carrie Devers, Theresa Culver, Amy Capodici, Georgeann Roberts, and Pamela Silver ("Plaintiffs"), on behalf of themselves and all others similarly situated, through undersigned counsel, bring this Consolidated Class Action against Defendant Onsite Mammography, LLC, d/b/a Onsite Women's Health ("Defendant" or "Onsite") and allege, upon personal knowledge as to their own actions and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this action because Onsite failed to properly secure and safeguard their personally identifiable information ("PII") and protected health information ("PHI") and that of more than 350,000 current and former patients

(collectively, the "Class" or "Class Members"). The compromised data include names, Social Security numbers, dates of birth, driver's license numbers, credit card numbers, and sensitive medical information concerning patients' mental or physical conditions and the care they received (collectively, the "Private Information").

2. Onsite is a limited-liability company incorporated under the laws of Connecticut and headquartered in Massachusetts, where it operates in-office breast imaging services nationwide under the "Onsite Women's Health" brand.

3. On or about October 2024, Onsite discovered that a threat actor had gained unauthorized access to a single employee's e-mail account through a phishing attack, thereby accessing and exfiltrating messages and attachments containing patient data (the "Data Breach"). In their Notice of Data Breach (the "Notice"), Defendant states:

> In October 2024, we discovered unusual activity associated with one employee's email account. After taking immediate steps to ensure our email environment was secure, we enlisted independent cybersecurity experts to conduct an investigation to determine what happened and whether sensitive information may have been impacted. According to the investigation, an unauthorized actor gained access to the individual's email account for a brief window of time. Due to the nature of some of the emails in this employee's inbox, we engaged the services of an outside data analytics vendor, that conducted a comprehensive review of the impacted files to determine whether any PHI was involved. The investigation further revealed that the actor only had access to the email account and did not have access to any other systems within our network. The data analytics vendor's review concluded on February 21, 2025, and revealed that the compromised email included specific health-related information about patients.[1]

[1] *See Notice of Data Breach*, https://www.maine.gov/cgi-bin/agviewerad/ret?loc=2397.

4. Plaintiffs and Class Members now face a substantial and imminent risk of identity theft, medical identity fraud, unauthorized credit card use, and other personal, social, and financial harms that may persist for life.

5. Armed with the stolen Private Information, cybercriminals can, inter alia, obtain medical services or prescriptions, open financial accounts, take out loans, file fraudulent tax returns, or obtain identification documents in Class Members' names.

6. Onsite has offered 12 months of complimentary Equifax Credit Watch Gold but has provided no assurance that all copies of the data have been recovered or destroyed, nor that its data security posture has been sufficiently strengthened.

7. Plaintiffs and Class Members therefore suffered, and continue to suffer, ascertainable losses, including heightened risk of identity theft, out-of-pocket mitigation costs, lost time, and diminished value of their Private Information, which has independent economic value in the marketplace and has been rendered less secure and thus less valuable by Defendant's conduct.

8. Plaintiffs seek redress for Onsite's inadequate safeguarding of Class Members' Private Information.

9. Onsite failed to implement reasonable security measures commensurate with the sensitivity of the data it held.

10. Had adequate safeguards been in place, Onsite would have prevented—or at least detected far earlier—the unauthorized access.

11. Plaintiffs' and Class Members' identities were compromised solely because of Onsite's negligent conduct.

12. Plaintiffs bring this action on behalf of themselves and all similarly situated individuals whose Private Information was exfiltrated during the Data Breach.

13. Onsite's disclosures omit critical facts, including the precise duration of unauthorized access, the complete set of data elements stolen, and the reasons for the protracted delay in notification—thus hampering victims' mitigation efforts.

14. Without these details, Plaintiffs' and Class Members' ability to protect themselves has been severely diminished

15. As a direct and proximate result of Onsite's deficient security practices, Plaintiffs' and Class Members' Private Information is now in the hands of cybercriminals.

16. Because their data is already in the hands of cybercriminals, Plaintiffs and Class Members face an impending risk of fraud, identity theft, misuse of health-insurance benefits, intrusion upon health privacy, and dissemination of their data on the dark web.

17. Plaintiffs have suffered and continue to suffer present, concrete injuries that exist independent of any future identity theft, including:

a. Loss of the value of their Private Information, which has been taken from them without consent;

b. Time already spent and being spent addressing the Data Breach—time that has been lost forever and cannot be recaptured;

c. Out-of-pocket costs already incurred for protective measures; and

d. Present anxiety and emotional distress of knowing their most sensitive information is in criminal hands.

18. Plaintiffs and Class Members must now devote additional time, money, and effort to monitor their accounts, secure credit files, and otherwise protect themselves. These injuries are concrete, particularized, and either have already occurred or are certainly impending given that Plaintiffs' data is now in the hands of cybercriminals who specifically targeted it.

19. On behalf of the Class, Plaintiffs assert claims for (i) Negligence; (ii) Breach of Implied Contract; (iii) Breach of Fiduciary Duty; (iv) Invasion of Privacy; (v) Unjust Enrichment; and (vi) Declaratory Judgment. Plaintiffs seek damages and injunctive relief, including Court-ordered implementation of industry standard information security measures, regular security audits, and long-term identity theft protection services to prevent future breaches.

PARTIES

20. Plaintiff Rose Clarkson is, and at all times relevant hereto was, a citizen of the State of West Virginia, residing in Union, West Virginia.

21. Plaintiff June Mack is, and at all times relevant hereto was, a citizen of Alabama, residing in Clanton.

22. Plaintiff Valerie Hicks is, and at all times relevant hereto was, a citizen of North Carolina, residing in Garner.

23. Plaintiff Carrie Devers is, and at all times relevant hereto was, a citizen of Alabama residing in Elba.

24. Plaintiff Theresa Culver is, and at all times relevant hereto was, a citizen of Virginia, residing in Norfolk.

25. Plaintiff Amy Capodici is, and at all times relevant hereto was, a citizen of Pennsylvania, residing in Wayne.

26. Plaintiff Georgeann Roberts, and at all times relevant hereto was, a citizen of Virginia, residing in Charlottesville.

27. Plaintiff Silver, and at all times relevant hereto was, a citizen of Texas, residing in Dallas.

28. Defendant Onsite Mammography, LLC is a Connecticut limited liability company with its principal place of business and corporate headquarters located at 815 North Road, Westfield, Massachusetts 01085.

JURISDICTION & VENUE

29. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, the proposed Class contains more than 100 members, and Plaintiffs and many Class Members are citizens of states different from Defendant.

30. This Court has personal jurisdiction over Defendant because it is headquartered in this District, transacts substantial business here, and many of the wrongful acts and omissions alleged in this herein emanated from this District.

31. Venue is proper in this Court under 28 U.S.C. § 1391(b)(1)–(2) because Defendant resides in this District, and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' and the Class's claims occurred in this District.

COMMON FACTUAL ALLEGATIONS

A. Defendant Collects a Significant Amount of Private Information.

32. Plaintiffs and Class Members are current and former patients who received medical imaging and diagnostic services from Onsite.

33. In order to receive those services, patients—including Plaintiffs and Class Members—were required to provide Onsite with sensitive Private Information.

34. Upon information and belief, Onsite represented—through its HIPAA Notice of Privacy Practices, website privacy policy, and other statutory disclosures—that it would maintain that information in strict confidence and employ reasonable safeguards to protect it.

35. Given the highly sensitive nature of the information it collects, Onsite is obligated to (a) keep patients' Private Information confidential; (b) follow industry-standard data security practices; (c) inform patients of its data security duties; (d) comply with all applicable federal and state privacy laws; (e) use or disclose the data only for legitimate medical or administrative purposes; and (f) provide prompt notice of any unauthorized disclosure.

36. By obtaining and benefiting from Plaintiffs' and Class Members' Private Information, Onsite assumed legal and equitable duties to protect that data from unauthorized access or disclosure.

37. Without the submission of such data, Onsite could not perform the imaging and diagnostic services it offers.

38. Plaintiffs and Class Members reasonably relied on Onsite to maintain their

Private Information securely and to disclose it only as authorized. Onsite ultimately failed to honor these duties.

39. According to the Notice, Onsite discovered unusual activity associated with one employee's email account in October 2024, and a forensic investigation revealed that an unauthorized actor gained access to the individual's email account for a brief window of time, during which patient data were exposed.[2]

40. Onsite engaged an outside data analytics vendor whose review "concluded on February 21, 2025, and revealed that the compromised email included specific health-related information about patients."[3]

41. Defendant reported that the following information may have been compromised in the Data Breach: contact details such as names, addresses, phone numbers, and email addresses; medical/clinical information (including date(s) of service, diagnoses, treatments, medical record numbers, lab results, patient/accession numbers, provider names, and treatment locations); health insurance information (including plan names, plan types, insurance companies, and member/group ID numbers); billing, claims, and payment data (including bank account details and payment card details); and additional identifiers such as Social Security Numbers, driver's license or state ID numbers, passport numbers, and dates of birth.

42. Despite having completed its internal review of the Data Breach on February 21, 2025, Onsite did not begin issuing notice letters until mid-April 2025,

[2] *Id.*
[3] *Id.*

leaving a gap of nearly two months during which Plaintiffs and Class Members were unaware that their Private Information had been compromised.

43. Astonishingly, Defendant is attempting to shift responsibility for its failure to protect Plaintiffs' and Class Members' Private Information to the victims of the Data Breach, stating in its Notice, "[a]s a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained."[4]

44. The gap between the October 2024 breach and Defendant's delayed notification in April 2025 is itself evidence of concrete injury because Plaintiffs were deprived of the ability to take protective measures while criminals had unfettered use of their information. This deprivation of the opportunity for timely mitigation is an independent injury to Plaintiffs.

45. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information.

46. The unauthorized party accessed and acquired files in Defendant's systems containing unencrypted Private Information of Plaintiffs and Class Members. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

[4] *Id.*

B. Defendant Knew the Risks of Storing Valuable Private Information & the Foreseeable Harm to Victims.

47. Defendant is well aware that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

48. Defendant also knew that a breach of its systems—and exposure of the information stored therein—would result in the increased risk of identity theft and fraud (financial and medical) to the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

49. These risks are not merely theoretical; in recent years, numerous high-profile data breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, and Anthem as well as countless ones in the healthcare industry.

50. PII has considerable value and constitutes an enticing and well-known target to hackers, who can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[5]

51. PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.[6]

52. The prevalence of data breaches and identity theft has increased

---

[5] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited Aug. 29, 2025).

[6] *See* Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited Aug. 29, 2025).

dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities.

53. In 2021 alone, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[7]

54. 2024 was the worst-ever year in terms of breached healthcare records, which jumped by 64.1% from last year's record-breaking total to 276,775,457 breached records, or 81.38% of the 2024 population of the United States.

55. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years; for instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[8]

56. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[9]

57. Additionally, healthcare providers "store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly –

---

[7] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://go.flashpoint-intel.com/docs/2021-Year-End-Report-data-breach-quickview (last visited Aug. 29, 2025).

[8] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Aug. 29, 2025).

[9] *The healthcare industry is at risk*, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Aug. 29, 2025).

making the industry a growing target."[10]

58. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[11]

59. The healthcare sector suffered about 337 breaches in the first half of 2022 alone according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percent in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[12]

60. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud and more.

61. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "[m]edical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI

---

[10] *Id.*

[11] *2022 Breach Barometer*, https://www.protenus.com/breach-barometer-report (last visited Aug. 29, 2025).

[12] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited Aug. 29, 2025).

records can go from $20 say up to—we've even seen $60 or $70."[13]

62. A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market whereas stolen payment card information sells for about $1.[14] According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[15]

---

[13] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited Aug. 29, 2025).

[14] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Aug. 29, 2025).

[15] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited Aug. 29, 2025).

63. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security Number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

64. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

65. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

66. For these reasons, the FTC recommends that identity theft victims take several time consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[16] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

67. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

68. For example, Social Security numbers, which were compromised in the Data Breach, are among the worst type of information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then,

[16] *See* https://www.identitytheft.gov/Steps (last visited Aug. 29, 2025).

> they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

69. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

70. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

71. There may be a substantial time lag between when harm from a data breach occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused.

72. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held

---

[17] *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 29, 2025).

[18] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back* (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Aug. 29, 2025).

for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[19]

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

74. Based on the value of its patients' Private Information to cybercriminals, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. The Data Breach was Preventable.

75. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information Defendant collected from and maintained for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer

[19] *Report to Congressional Requesters, Personal Information* (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 29, 2025).

needed.

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

77. As a result of Defendant's inadequate training and supervision of its IT and data security agents and employees, failure to implement reasonable security measures and breach of its legal duties and obligations, the aforementioned Data Breach occurred, and Plaintiffs' and Class Members' Private Information was accessed and "stolen" by an unspecified "bad actor." Defendant permitted Plaintiffs' and Class Members' Private Information to be held in unencrypted form despite the heightened sensitivity of such Private Information.

78. To prevent and detect cyber-attacks and/or phishing attacks, Defendant could and should have implemented numerous measures as recommended by the United States Government, including but not limited to:

- Implementing an awareness and training program.
- Enabling strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scanning all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configuring firewalls to block access to known malicious IP addresses.
- Setting anti-virus and anti-malware programs to conduct regular scans automatically.

- Managing the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.[20]

79. Given that Defendant was storing the PII and PHI of its current and former patients and customers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

80. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of more than three hundred and fifty thousand people, including that of Plaintiffs and Class Members.

D. Defendant is Obligated Under HIPAA to Safeguard Private Information.

81. Defendant is required by HIPAA to safeguard patient PHI.

82. Defendant is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

83. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

84. Further to 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is

[20] How to Protect Your Networks from RANSOMWARE, at 3, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited August 29, 2025).

"transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

85. Under C.F.R. 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) "either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

86. HIPAA requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

87. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[21]

[21] *Breach Notification Rule*, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Aug. 29, 2025).

88. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiffs or the Class Members consent to the disclosure of their PHI to cybercriminals.

89. As such, Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and Class Members' PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

90. Given the application of HIPAA to Defendant, and that Plaintiffs and Class Members entrusted their PHI to Defendant in order to receive healthcare services, Plaintiffs and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

E. FTC Guidelines Prohibit Defendant from Engaging in Unfair or Deceptive Acts or Practices.

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

92. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the

FTC, the need for data security should be factored into all business decision-making.[22]

93. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[23]

94. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.[24]

95. The FTC has brought enforcement actions against businesses 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 FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[22] *Start with Security – A Guide for Business* (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Aug. 29, 2025)

[23] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 29, 2025)

[24] *Id.*

96. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

97. Defendant was at all times fully aware of its obligations to protect the PII and PHI of patients because of its position as a healthcare provider, which gave it direct access to reams of patient Private Information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Defendant Violated Industry Standards.

98. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of PII and PHI, like Defendant, including but not limited to: educating all employees; vetting all vendors; using strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data.

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

100. Defendant failed to meet the minimum standards of any of the following

frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

G. The Monetary Value of Plaintiff's & Class Members' Private Information.

102. As a result of Defendant's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

103. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identifying fraud is only about 3%.[25]

104. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly

[25] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Aug. 29, 2025).

remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[26]

105. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[27]

106. Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

107. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[28]

108. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[29]

---

[26] *Id.*

[27] Andrew Steger, *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Aug. 29, 2025).

[28] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited Aug. 29, 2025).

[29] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy* (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274 (last visited Aug. 29, 2025).

109. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[30]

110. Recognizing the high value that consumers place on their PII and PHI, many companies now offer consumers an opportunity to sell this information.[31] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their PII and PHI. This business has created a new market for the sale and purchase of this valuable data.

111. Consumers place a high value not only on their PII and PHI, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[32]

112. The value of Plaintiffs' and Class Members' PII and PHI on the black

---

[30] *Statement of FTC Commissioner Pamela Jones Harbour – Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited Aug. 29, 2025).

[31] Angwin & Steel, *supra* note 32.

[32] *See* U.S. Dep't of Justice, *Victims of Identity Theft* (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Aug. 29, 2025).

market is substantial. Sensitive health information can sell for as much as $363.[33]

113. This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can also be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or to gain access to prescriptions for illegal use or resale.

114. Health information, in particular, is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[34]

115. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[35]

116. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World

---

[33] *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited Aug. 29, 2025).
[34] *Id.*
[35] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, https://www.experian.com/innovation/thought-leadership/medical-identity-theft-healthcare-data-breaches.jsp (last visited Aug. 29, 2025).

Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[36]

117. The FTC has warned consumers of the dangers of medical identity theft, stating that criminals can use personal information like a "health insurance account number or Medicare number" to "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." The FTC further warns that instances of medical identity theft "could affect the medical care you're able to get or the health insurance benefits you're able to use[,]" while also having a negative impact on credit scores.[37]

118. Here, where health insurance information was among the PII and PHI impacted in the Data Breach, Plaintiffs' and Class Members' risk of suffering future medical identity theft is especially substantial.

119. The ramifications of Defendant's failure to keep its patients' PII and PHI secure are long-lasting and severe. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for 6 to 12 months or even longer.

120. Approximately 21% of victims do not realize their identity has been

---

[36] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/ (last visited Aug. 29, 2025).
[37] *What to Know About Medical Identity Theft*, What To Know About Medical Identity Theft | Consumer Advice (ftc.gov) (last visited Aug. 29, 2025).

compromised until more than two years after it has happened.[38] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[39]

121. Indeed, when compromised, healthcare-related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[40]

122. Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft, including medical identity theft, have a crippling effect on individuals and detrimentally impact the

---

[38] *See Medical ID Theft Checklist*, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Aug. 29, 2025).

[39] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches* (Apr. 18010), https://www.experian.com/innovation/thought-leadership/medical-identity-theft-healthcare-data-breaches.jsp (last visited Aug. 29, 2025).

[40] Elinor Mills, *Study: Medical identity theft is costly for victims* (March 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited Aug. 29, 2025).

economy as a whole.[41]

123. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the PII and PHI it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft (including medical identity theft) and fraud.

124. Upon information and good faith belief, had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented the phishing attack into its systems and, ultimately, the theft of the PII and PHI of patients within its systems.

125. The compromised PII and PHI in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves.

126. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[42] For example, different PII elements from various sources may be able to be

---

[41] *Id.*

[42] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, at 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework (last visited Aug. 29, 2025).

linked in order to identify an individual, or access additional information about or relating to the individual.[43]

127. Upon information and belief, the unauthorized parties have already utilized, and will continue to utilize, the PII and PHI they obtained through the Data Breach to obtain additional information from Plaintiffs and Class Members that can be misused.

128. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

129. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' PII and PHI to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

130. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' PII and PHI has thus deprived customers of the full monetary value of their transaction with the company.

131. In short, the data exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

H. Plaintiffs & Class Members Have Suffered Compensable Damages.

[43] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

132. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways.

133. The risks associated with identity theft, including medical identity theft, are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

134. In order to mitigate the risks of identity theft and fraud, Plaintiffs and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

135. Once PII and PHI are exposed, there is virtually no way to ensure that the exposed information has been fully recovered or protected against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

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

137. Plaintiffs and Class Members now face a greater risk of identity theft, including medical and financial identity theft.

138. Plaintiffs now live with the ongoing reality that their information is in criminal hands. This is an ongoing injury that cannot be undone, and each day that passes with Plaintiffs' and Class Members' information outside their control represents a continuation of the original injury.

139. Establishing injury here does not require a speculative chain of possibilities. The causal chain is direct and simple: (1) Defendant collected and stored Plaintiffs' most sensitive information; (2) Defendant failed to adequately protect it; (3) cybercriminals successfully stole it through a targeted attack; and (4) Plaintiffs must now expend time and money to protect themselves and face a substantially increased risk of identity theft. Each link in this chain has already occurred.

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

141. Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

142. Plaintiffs and Class Members also did not receive the full benefit of their bargain when paying for medical services. Instead, they received services of a diminished value to those described in their agreements with Defendant. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

143. Plaintiffs specifically relied on Defendant's HIPAA-mandated obligations to safeguard their PHI when choosing to receive medical services. The federal statutory framework created reasonable expectations of data security that formed a material part of the parties' bargain. Plaintiffs paid for services that included HIPAA-compliant data protection but received services with substandard security, representing a concrete economic injury measured by the difference in value.

144. Plaintiffs and Class Members would not have obtained services from Defendant had they known that Defendant failed to implement proper data security practices to safeguard their PII and PHI from criminal theft and misuse.

145. Plaintiffs contracted for medical services that included, as an integral component, the safeguarding of their highly sensitive medical information pursuant to HIPAA and industry standards. In receiving medical services coupled with inadequate data security that lead to exposed them to lifelong risks, they received something of substantially less value than what they bargained for.

146. Finally, in addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their PII and PHI

remain secure and are not subject to further misappropriation and theft.

REPRESENTATIVE PLAINTIFFS' EXPERIENCE

Plaintiff Rose Clarkson

147. Plaintiff Clarkson was a patient at one of Defendant's clinics in or around September-October 2024.

148. As a condition of obtaining services from Defendant, she was required to provide her PII and PHI to Defendant.

149. Upon information and good faith belief, Defendant maintained Plaintiff Clarkson's PII and PHI in its systems at the time of the Data Breach.

150. On or about April 21, 2025, Plaintiff Clarkson received a notice of the Data Breach notifying her that her PII and PHI was impacted by this Data Breach.

151. Plaintiff Clarkson is very careful about sharing her sensitive PII and PHI. She stores any documents containing PII or PHI in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff Clarkson would not have entrusted her PII or PHI to Defendant had she known of Defendant's lax data security policies.

152. As a result of the Data Breach, Plaintiff Clarkson made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial accounts for any unusual activity, which may take years to detect. Plaintiff Clarkson has spent significant time dealing with the Data Breach, including having to change her debit car due to fraudulent activity – valuable

time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

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

154. Plaintiff Clarkson additionally suffered actual injury in the form of her PII and PHI being disseminated, on information and belief, on the dark web as a result of the Data Breach.

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

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

157. Plaintiff Clarkson has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff June Mack's Experience

158. Plaintiff Mack was a patient of Defendant at one of Defendant's clinics.

159. As a condition of obtaining services from Defendant, she was required to provide her PII and PHI to Defendant.

160. Upon information and belief, Defendant maintained Plaintiff Mack's PII and PHI in its systems at the time of the Data Breach.

161. Plaintiff Mack received a Notice Letter, by U.S. mail, directly from Defendant, dated April 21, 2025. According to the Notice Letter, Plaintiff Mack's PII and PHI was improperly accessed and obtained by unauthorized third parties.

162. Plaintiff Mack is very careful about sharing her sensitive PII and PHI. She stores any documents containing PII or PHI in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff Mack would not have entrusted her PII or PHI to Defendant had she known of Defendant's lax data security policies.

163. As a result of the Data Breach, Plaintiff Mack made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial accounts for any unusual activity, which may take years to detect.

164. Plaintiff Mack has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

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

166. Plaintiff further suffered actual injury in the form of experiencing an excessive number of spam and harassing calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. These communications are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls and texts are related to her stolen PII.

167. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

168. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed Plaintiff of key details about the Data Breach's occurrence.

169. Plaintiff Mack additionally suffered actual injury in the form of her PII and PHI being disseminated, on information and belief, on the dark web as a result of the Data Breach.

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

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

172. Plaintiff Mack has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Valarie Hicks' Experience

173. Plaintiff Hicks is and was Defendant's patient at all times relevant to this Complaint. Plaintiff Hicks received a Notice of Data Breach Letter, related to Defendant's Data Breach, dated April 21, 2025.

174. The Notice Letter that Plaintiff Hicks received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her name, "Social Security numbers, dates of birth, driver's license numbers, credit card numbers, and medical information such as mental and physical health or condition and received care information."

175. Plaintiff Hicks is especially alarmed by the vagueness in the Notice Letter regarding her stolen extremely private medical information, including her PII/PHI, as among the breached data on Defendant's computer system.

176. Since the Data Breach, Plaintiff Hicks has tried to mitigate the damage by changing her passwords, contacting the credit bureaus as Defendant instructed, and monitoring her financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time as a result of Defendant's negligence, but it also causes her great anxiety.

177. Soon after the Data Breach, Plaintiff Hicks began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen PII.

178. Plaintiff Hicks is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

179. Plaintiff Hicks has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

180. Plaintiff has experienced anxiety and increased concerns arising from the fact that her Private Information has been or will be misused and from the loss of her privacy.

181. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names, dates of birth, and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

182. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such will include future costs and expenses.

183. Plaintiff has a continuing interest in ensuring that her PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

184. Had Plaintiff Hicks been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

Plaintiff Carrie Devers' Experience

185. Plaintiff Carrie Devers is and was a patient of Defendant at one of Defendant's clinics. Plaintiff Devers came to Defendant for healthcare services and, in order to receive services, Defendant required Devers to provide her Private Information to Defendant.

186. Plaintiff Devers received notice of the Data Breach around April 21, 2025, informing her that her sensitive information was part of Defendant's Data Breach. After the date of the Data Breach, Plaintiff Devers was informed that some of her Private Information could be found on the Dark Web, which she attributed to Defendant's Data Breach as she was informed shortly after the Data Breach occurred in the first of the year 2025.

187. Plaintiff Devers reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard her Private Information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to the same.

188. Devers is very careful about sharing her sensitive PII and PHI. she has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any

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

189. Because of the Data Breach and at the recommendation of Defendant and its Notice, Plaintiff Devers made reasonable efforts to mitigate the effect of the Data Breach, including, but not limited to, researching the Data Breach, reviewing financial statements, monitoring her credit information, and changing passwords on her various accounts.

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

191. Plaintiff Devers has spent much time responding to the dangers from the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and recreation.

192. Plaintiff Devers is especially alarmed by the amount and type of stolen or accessed PII and PHI listed on Defendant's notice letter. Despite Defendant providing that list, she cannot be sure whether more of her PII or PHI was exfiltrated.

193. Plaintiff Devers knows that cybercriminals often sell Private Information, and that her PII or PHI could be abused months or even years after a data breach.

194. Plaintiff Devers would not have provided her Private Information to Defendant had she known that Defendant would not take reasonable steps to safeguard it. Devers has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Theresa Culver's Experience

195. Upon information and belief, Defendant obtained Plaintiff Culver's Private Information in the course of conducting its regular business operations.

196. At the time of the Data Breach–in or around October 2024–Defendant retained Plaintiff Culver's Private Information in its system.

197. Plaintiff Culver received the Notice Letter, by U.S. mail, directly from Defendant, dated April 21, 2025. According to the Notice Letter, Plaintiff's PII and PHI was improperly accessed and obtained by unauthorized third parties.

198. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff to "remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the FTC." Plaintiff Culver made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff Culver has spent significant time dealing with the Data Breach--valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

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

Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

200. Plaintiff Culver additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices by phishing attacks or elicit further personal information for use in committing identity theft or fraud.

201. The Data Breach has caused Plaintiff Culver to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed Plaintiff Culver of key details about the Data Breach's occurrence.

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

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

204. Plaintiff Culver has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Amy Capodici's Experience

205. Plaintiff Capodici was a patient at one of Defendant's clinics.

206. As a condition of obtaining services from Defendant, she was required to provide her PII and PHI to Defendant.

207. Upon information and good faith belief, Defendant maintained Plaintiff Capodici's PII and PHI in its systems at the time of the Data Breach.

208. On or about April 21, 2025, Plaintiff Capodici received a notice of the Data Breach notifying her that her PII and PHI was impacted by this cyber incident.

209. Plaintiff Capodici is very careful about sharing her sensitive PII and PHI. She stores any documents containing PII or PHI in a safe and secure location. Plaintiff Capodici has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff Capodici would not have entrusted her PII or PHI to Defendant had she known of Defendant's lax data security policies.

210. As a result of the Data Breach, Plaintiff Capodici made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial accounts for any unusual activity, which may take years to detect. Plaintiff Capodici has spent significant time dealing with the Data Breach, including having to change her debit car due to fraudulent activity - valuable

time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

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

212. Plaintiff Capodici additionally suffered actual injury in the form of her PII and PHI being disseminated, on information and belief, on the dark web as a result of the Data Breach.

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

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

215. Plaintiff Capodici has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Georgann Roberts' Experience

216. Plaintiff Roberts has been a mammography patient at Sentara Hospital in Charlottesville, VA for over 25 years, and Sentara Hospital utilizes Onsite Mammography imaging services.

217. As a condition of obtaining services from Defendant, she was required to provide her PII and PHI to Defendant.

218. Upon information and good faith belief, Defendant maintained Plaintiff Roberts's PII and PHI in its systems at the time of the Data Breach.

219. On or about April 21, 2025, Plaintiff Roberts received a notice of the Data Breach notifying her that her PII and PHI was impacted by this cyber incident.

220. Plaintiff Roberts is very careful about sharing her sensitive PII and PHI. She stores any documents containing PII or PHI in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff Roberts would not have entrusted her PII or PHI to Defendant had she known of Defendant's lax data security policies.

221. As a result of the Data Breach, Plaintiff Roberts has and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent verifying the legitimacy of communications related to the Data Breach, and self-

monitoring her accounts and reviewing her credit report after the Data Breach to ensure no fraudulent activity has occurred.

222. This is valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

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

224. Plaintiff Roberts additionally suffered actual injury in the form of her PII and PHI being disseminated, on information and belief, on the dark web as a result of the Data Breach.

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

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

227. Plaintiff Roberts has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Silver's Experience

228. Plaintiff Silver is a mammography patient at Women's Specialists of Plano in Plano, Texas, and Women's Specialists utilizes Onsite Mammography imaging services.

229. As a condition of obtaining services from Defendant, Plaintiff Silver was required to provide her PII and PHI to Defendant.

230. Upon information and good faith belief, Defendant maintained Plaintiff Silver's PII and PHI in its systems at the time of the Data Breach.

231. Defendant sent Plaintiff Silver a notice of the Data Breach, dated April 21, 2025, notifying her that her PII and PHI was impacted by this cyber incident.

232. Plaintiff Silver is very careful about sharing her sensitive PII and PHI. She stores any documents containing PII or PHI in a safe and secure location. Plaintiff Silver has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or

any other unsecured source. Plaintiff Silver would not have entrusted her PII or PHI to Defendant had she known of Defendant's lax data security policies.

233. As a result of the Data Breach, Plaintiff Silver has and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent verifying the legitimacy of communications related to the Data Breach, and self-monitoring her accounts and reviewing her credit report after the Data Breach to ensure no fraudulent activity has occurred.

234. This is valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

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

236. Plaintiff Silver additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her PII and PHI was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

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

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

239. Plaintiff Silver has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

240. Plaintiffs bring this class action on behalf of themselves and all other individuals who are similarly situated for the Class defined below, pursuant to Fed. R. Civ. P 23.

241. Plaintiffs seek to represent a Nationwide Class of persons to be defined as follows:

> All individuals residing in the United States whose Private Information was compromised in the Data Breach that was reported by Defendant in April 2025.

242. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families, all judges assigned to hear any aspect of this litigation, their immediate family members, and those individuals who make a timely and effective election to be excluded from this matter using the correct protocol for opting out.

243. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

244. **Numerosity** (Fed. R. Civ. P. 23(a)(1)): The proposed class is so numerous that joinder of all members is impracticable. Plaintiffs are informed and believe, and thereon allege, that there are, at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are ascertainable through Defendant's records, including but not limited to the files and records related to the Data Breach.

245. **Commonality** (Fed. R. Civ. P. 23(a)(2)): This action involves questions of law and fact common to the Class that predominate over any questions affecting solely individual members of the Class. Such common questions include but are not limited to:

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

b. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

c. Whether and when Defendant actually learned of the Data Breach;

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

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

f. Whether Defendant violated federal law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

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

h. Whether Defendant adequately addressed and fixed the vulnerabilities that allowed the Data Breach to occur;

i. Whether Defendant's negligence resulted in the Data Breach;

j. Whether Defendant entered into an implied contract with Plaintiffs and Class Members;

k. Whether Defendant breached that contract by failing to adequately safeguard Plaintiffs' and Class Members' Private Information;

l. Whether Defendant was unjustly enriched;

m. Whether Plaintiffs and Class Members are entitled to actual, statutory, and/or nominal damages as a result of Defendant's wrongful conduct; and

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

246. **Typicality** (Fed. R. Civ. P. 23(a)(3)): Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class had all sought and/or received services from Defendant, each having their Private Information exposed and/or accessed by an unauthorized third party.

247. **Adequacy of Representation** (Fed. R. Civ. P. 23(a)(4)): Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the members of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and have no interests antagonistic to the members of the Class. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above.

248. **Superiority**: This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than

individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

249. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device particularly efficient and appropriate to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

250. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

251. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth herein.

252. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory

relief are appropriate on a class- wide basis.

253. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiffs and the Class of the Data Breach;

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

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

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard patient Private Information; and

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

254. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant breached its duty to Plaintiffs and Class Members, then Plaintiff and each Class member suffered damages

by that conduct.

255. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class.

256. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

CAUSES OF ACTION

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

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

258. Plaintiffs bring this claim individually and on behalf of the Class.

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

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

261. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By

collecting and storing valuable Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

262. Defendant's duty also arose from its position as healthcare provider. Defendant holds itself out as trusted providers of healthcare and thereby assumes a duty to reasonably protect its patients' information.

263. Defendant breached the duties owed to Plaintiffs and Class Members and thus was negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiffs' and Class Members' Private Information, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Private Information;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of key controls, systems, and procedures;

e. failing to evaluate and adjust its information security requirements in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to their

patients regarding its oversight; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

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

265. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. The diminished value of the services they paid for and received, and

k. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

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

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

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

268. Plaintiffs bring this claim individually and on behalf of the Class.

269. When Plaintiffs and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiffs' and Class Members' Private Information, comply with its statutory and common law duties to protect Plaintiffs' and Class Members' Private Information, and to timely notify them in the event of a data

breach.

270. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's provision of healthcare services. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

271. Implicit in the agreement between Plaintiffs and Class Members and Defendant was Defendant's obligation to:

a. use such Private Information for business purposes only;

b. take reasonable steps to safeguard Plaintiffs' and Class Members' Private Information;

c. prevent unauthorized access and/or disclosure of Plaintiffs' and Class Members' Private Information through proper monitoring and oversight;

d. provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their Private Information, whether through Defendant's systems;

e. reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized access and/or disclosure at all points of collection, storage, and use; and

f. ensure that Plaintiffs' and Class Members' Private Information is retained under conditions that kept such information secure and confidential by both Defendant and any third parties with whom Defendant shares such information.

272. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with their statutory and common law duties to adequately protect Plaintiffs' and Class Members' Private Information and to timely notify them in the event of a data breach.

273. Plaintiffs and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their Private Information from unauthorized access and disclosure, regardless of whether such information was stored on Defendant's systems. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security and to properly vet, monitor, and oversee any system holding patient information. Defendant failed to do so.

274. Plaintiffs and Class Members would not have provided their Private Information to Defendant had they known that Defendant would not adequately safeguard their Private Information as promised.

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

276. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard their Private Information, failing to implement reasonable security measures, and failing to provide them with timely and accurate notice of the Data Breach.

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

278. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard their Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

279. The losses and damages Plaintiffs and Class Members sustained, include,

but are not limited to:

a. Theft of their PII and/or PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of Private

Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

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

281. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strengthen its data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) immediately provide and continue to provide adequate credit monitoring to Plaintiffs and all Class Members.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

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

283. Given the relationship between Defendant and Plaintiffs and Class Members, where Defendant became guardian of Plaintiffs' and Class Members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' PII/PHI; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

284. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class

Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

285. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices, such as Defendant's sharing Private Information with insufficiently secured third parties.

286. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently protect Plaintiffs' and Class Members' PII/PHI.

287. Defendant also breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

288. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

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

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

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

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

292. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class Members' PII/PHI is highly offensive to a reasonable person.

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

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

295. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices (including partnerships and data-sharing agreements with insufficiently secure third parties) were inadequate.

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

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

298. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiffs and the Class was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

299. On information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

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

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

302. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

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

303. Plaintiffs restate and reallege all preceding factual allegations above as if

fully set forth herein, and pleads the following count in the alternative.

304. Plaintiffs bring this claim individually and on behalf of the Class.

305. Upon information and belief, Defendant funded its data security measures and data-sharing agreements from its general revenue including payments made by or on behalf of Plaintiffs and Class Members.

306. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

307. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased healthcare services from Defendant and/or its agents and in so doing provided Defendant with their Private Information.

308. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

309. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

310. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members Private Information. Instead of providing a reasonable level of data security that would have prevented the Data Breach, Defendant instead calculated to increase

its own profits and the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective data security measures.

311. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

312. Defendant failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members conferred upon Defendant.

313. Defendant acquired Plaintiffs' and Class Members' Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

314. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

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

316. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

317. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and

other economic and noneconomic losses.

318. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT VI
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

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

320. Plaintiffs bring this claim individually and on behalf of the Class.

321. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described herein.

322. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs' and Class Members from further data breaches that compromise their Private Information. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and

remain at imminent risk that further compromises of their Private Information will occur in the future.

323. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure patients' PII and PHI and to timely notify patients of a data breach under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

324. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' Private Information.

325. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant's properties.

326. The risk of another such breach is real, immediate and substantial.

327. If another breach of Defendant's store of patient data occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

328. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of

complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

329. Issuance of the requested injunction will benefit the public by preventing another data breach at Defendant's facilities, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Rose Clarkson, June Mack, Valerie Hicks, Carrie Devers, Theresa Culver, Amy Capodici, Georgeann Roberts and Pamela Silver, on behalf of themselves and other Class Members, pray for judgment against Defendant Onsite Mammography, LLC, d/b/a Onsite Women's Health, and respectfully request that the Court issue an Order:

A. Certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. Awarding equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. Awarding injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

D. Awarding all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;

E. Awarding attorney fees, costs, and litigation expenses, as allowed by law;

F. Awarding prejudgment interest on all amounts awarded and

G. Awarding all such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and other members of the proposed Class, hereby demand a jury trial on all issues so triable.

Dated: September 4, 2025

Respectfully submitted,

/s/ John Roddy

John Roddy (BBO # 424240)
BAILEY & GLASSER LLP
101 Arch Street, 8th Floor
Boston, MA 02110
Tel: (617) 439-6730
Fax: (617) 951-3954
jroddy@baileyglasser.com

Interim Liaison Counsel

Elena A. Belov (admitted *pro hac vice)*
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (917) 716-7132
elena@almeidalawgroup.com

Jonathan S. Mann (admitted *pro hac vice)*
PITTMAN, DUTTON, HELLUMS, BRADLEY & MANN, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
jonm@pittmandutton.com

Marc H. Edelson (admitted *pro hac vice*)
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
Tel: (215) 867-2399
medelson@edelson-law.com

Interim Co-Lead Class Counsel

Leigh S. Montgomery*
ELLZEY KHERKHER SANFORD MONTGOMERY, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Tel: (888) 350-3931
lmontgomery@eksm.com

Marc S. Reich (admitted *pro hac vice*)
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Tel: (212) 363-7500
mreich@zlk.com

Jeff Ostrow (admitted *pro hac vice*)
KOPELOWITZ OSTROW P.A.
One West Las Olas Boulevard, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com

Leanna A. Loginov (admitted *pro hac vice*)
SHAMIS & GENTILE, P.A.
14 NE First Avenue, Suite 705
Miami, Florida 33132
Tel: 305-479-2299
lloginov@shamisgentile.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015
Tel: (866) 252-0878
dlietz@milberg.com

Plaintiffs' Executive Committee

Bart D. Cohen*
BAILEY & GLASSER LLP
1622 Locust Street
Philadelphia, PA 19103
Tel: (215) 274-9420
bcohen@baileyglasser.com

Additional Attorney for Plaintiffs and the Putative Classes

*** *Pro hac vice* forthcoming**