IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

JANE DOE, individually and on behalf of J.L., a minor child, and on behalf of all others similarly situated Plaintiffs, v. RADIOLOGY ASSOCIATES OF RICHMOND, INC., Defendant.	Case No: 3:25-cv-648 **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jane Doe ("Plaintiff"), individually, and on behalf of J.L., a minor child, and on behalf of all others similarly situated, brings this action against Defendant Radiology Associates of Richmond, Inc. ("Radiology Associates" or "Defendant") to obtain damages, restitution, and injunctive relief from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of their counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of Defendant Radiology Associates' failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiff's and Class Members' (defined below) sensitive personal identifiable information that it had acquired and stored for its business purposes.

2. Defendant is an organization that provides medical treatment and/or employment to individuals, including Plaintiff and Class Members. According to a "Notice of Data Security Incident" posted on Defendant's website, a data breach occurred in Radiology Associates' network

between April 2, 2024 through April 6, 2024, which was discovered on or about May 2, 2025 (the "Data Breach").[1]

3. Due to Defendant's data security failures which resulted in the Data Breach, cybercriminals were able to target Defendant's computer systems and exfiltrate Plaintiff's and Class Members' highly sensitive and personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information"). As a result of this Data Breach, Plaintiff's and Class Members' Private Information of remains in the hands of those cybercriminals. The website notice states that, upon learning of the Data Breach, Radiology Associates "[u]Upon learning of this issue, we immediately worked to contain the threat and secure our internal environment. After an extensive forensic investigation and complex manual document review, [Defendant] discovered on May 2, 2025 that the impacted systems, which were accessed between April 2, 2024 through April 6, 2024, contained identifiable protected health and personal information."[2]

4. However, despite apparently learning of the Data Breach on or about May 2, 2025 and determining that Private Information was involved in the breach, Defendant did not begin sending notices to the victims of the Data Breach (the "Notice of Data Security Incident Letters") until July 1, 2025.

5. The Private Information compromised in the Data Breach included current and former patients' PII and PHI, including Plaintiff's. This Private Information included, but is not limited to: patient names, 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

[1] https://rarichmond.com/notice-of-data-security-incident/ (last visited August 14, 2025)
[2] *Id.*

received care information.[3]

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiff's and Class Members' Private Information with which it was entrusted for either treatment or employment or both.

7. Plaintiff brings this class action lawsuit on behalf of herself and all other similarly situated persons to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and failing to include in that belated and inadequate notice precisely what specific types of information were accessed and taken by cybercriminals.

8. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that network in a dangerous condition.

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

[3] *Id.*

to prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and full notice of the Data Breach.

10. In addition, Defendant failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computer network and systems, it would have discovered the massive intrusion sooner rather than allowing cybercriminals almost a month of unimpeded access to the PII and PHI of Plaintiff and Class Members.

11. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

12. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including: opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

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

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

15. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all other similarly situated individuals whose Private Information was accessed during the Data Breach.

16. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of contract, (iii) breach of implied contract and (iv) breach of the implied covenant of good faith and fair dealing.

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

PARTIES

18. Plaintiff Jane Doe, individually and on behalf of the minor, J.L., is and at all times mentioned herein was an individual citizen of the State of Virginia, and was Defendant's patient. Plaintiff Jane Doe received notice of the Data Breach dated July 1, 2025, attached at Exhibit A.

19. Like Plaintiff, other potential Class members received similar notices informing them that their PII was exposed in the Data Breach on or about July 1, 2025.

20. Defendant Radiology Associates of Richmond, Inc. is a non-profit corporation with a principal place of business located in North Chesterfield, Virginia. Defendant operates provides a full range of imaging services including, general diagnostic, musculoskeletal, interventional, neuro-interventional, vascular, breast imaging, neuroradiology, cardiothoracic, pediatric and nuclear medicine.[4]

[4] https://rarichmond.com/about/ (last visited August 14, 2025).

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's state of citizenship.

22. This Court has personal jurisdiction over the parties in this case. Defendant Radiology Associates conducts business in this District and is a citizen of this District by virtue of having its principal place of business located in this District.

23. Venue is proper in this District under 28 U.S.C. §1391(b) because Radiology Associates maintains a headquarters in this District and regularly conducts business in this District.

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant Radiology Associates of Richmond, Inc. "provide[s] a full range of imaging services including, general diagnostic, musculoskeletal, interventional, neuro-interventional, vascular, breast imaging, neuroradiology, cardiothoracic, pediatric and nuclear medicine. Many of our physicians have additional training in highly specialized vascular and neurovascular specialties."[5]

25. For the purposes of this Class Action Complaint, all of Defendant's associated locations will be referred to collectively as "Defendant."

26. In the ordinary course of receiving medical care from Defendant, each patient must provide (and Plaintiff did provide) Defendant with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;

[5] https://rarichmond.com/about/ (last visited August 14, 2025).

- Date of birth;
- Social Security number;
- Marital status;
- Employer with contact information;
- Primary and secondary insurance policy holders' name, and address;
- Demographic information;
- Driver's license or state or federal identification;
- Information relating to the individual's medical and medical history;
- Insurance information and coverage; and
- Banking and/or credit card information.

27. Defendant also creates and stores medical records and other protected health information for its patients, records of treatments and diagnoses.

28. Upon information and belief, Defendant's HIPAA Notice of Privacy Practices ("Privacy Policy") is provided to every patient both prior to receiving treatment and upon request.[6] Defendant's Privacy Notice makes clear that it understands that its patients' Private Information is personal and must be protected by law.

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

30. Yet, through its failure to properly secure Plaintiff's and Class Members' Private Information, Defendant failed to meet its own promises of patient privacy.

[6] https://rarichmond.com/hipaa-privacy/ (last visited August 14, 2025).

31. The patient information held by Defendant in its computer system and network included Plaintiff's and Class Members' highly sensitive Private Information.

The Data Breach

32. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

33. According to its Data Breach Notice, it learned of a cyberattack on or about May 2, 2025, when an "n unauthorized actor gained access to its network environment."[7]

34. Defendant notified Department of Health and Human ("HHS") of the Data Breach on or about July 1, 2025, indicating a "hacking incident affected over 1.4 million individuals.[8]

35. Presently, however, Defendant has provided no public information on the ransom demand or payment.

36. In January 2023, two years before the attack, HHS created a presentation specifically for healthcare providers and IT departments, warning entities like Defendant of the severe threats posed by cybercriminal groups.[9] Within the healthcare industry, the risk of a cyberattack is well-known and preventable with adequate security systems in place.

37. On or about July 1, 2025, months after Defendant learned that the Class Members' Private Information was attacked by cybercriminals, Defendant's patients began receiving their notices of the Data Breach informing them that its investigation determined that their Private Information was accessed.

38. Defendant's notice letters list time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement

[7] *See* n.1, *supra*.
[8] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited August 14, 2025).
[9] https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf (last visited August 14, 2025).

about suspicious financial account activity. Also, Plaintiff would have to affirmatively sign up for and a call center number that victims may contact with questions. Defendant offered one year of credit monitoring for members of the class and Defendant offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves. On information and belief, Defendant sent a similar generic letter to all other individuals affected by the Data Breach.

39. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

40. Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

41. Defendant had obligations created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

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

43. It is well known that PII and PHI, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Defendant, are well-aware of the risk of being targeted by cybercriminals.

44. Individuals place a high value on the privacy of their PII and PHI. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

45. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, , or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[10]

46. Individuals, like Plaintiff and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing one's DNA for hacker's purposes.

47. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

48. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee

[10] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited August 14, 2025).

you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[11]

49. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches from 2020. Over the next two years, in a poll of security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable cases will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[12]

50. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

51. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [13] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[14]

52. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its

[11] https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited August 14, 2025).
[12] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last visited August 14, 2025).
[13] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited August 14, 2025).
[14] *Id.*

own acknowledgment of its duties to keep PII and PHI private and secure, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and the proposed Class from being compromised.

Data Breaches are Rampant in Healthcare.

53. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

54. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[15]

55. More than 144 million Americans' medical information was stolen or exposed during 2024.[16] This fact represents the continuation of record-breaking health care data breaches in the last several years. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[17]

56. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily

[15] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited August 14, 2025).
[16] *See* n.11, *supra*.
[17] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last visited August 14, 2025).

monetized."[18]

57. The HIPAA Journal article goes on to explain that patient records, like those stolen from Defendant, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[19]

58. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

59. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[20]

60. HHS data shows more than 39 million patients' information was exposed in the first half of 2023 in nearly 300 incidents and that healthcare beaches have doubled between 2020 and 2023, according to records compiled from HHS data by Health IT Security.[21]

61. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[22]

---

[18] *Id.*
[19] *Id.*
[20] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited August 14, 2025).
[21] https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far (last visited August 14, 2025).
[22] https://www.ahu.edu/blog/data-security-in-healthcare (last visited August 14, 2025).

62. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[23]

63. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant.

Defendant Failed to Comply with FTC Guidelines.

64. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

65. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[24] The guidelines also recommend that businesses use an intrusion detection

[23] Susan Henson, What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?, Experian (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-withyour-personal-information-and-how-can-you-protect-yourself/.

[24] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 14, 2025).

system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[25]

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

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

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

69. Defendant failed to properly implement basic data security practices.

70. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited

[25] *Id.*

by Section 5 of the FTC Act, 15 U.S.C. § 45.

71. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards.

72. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

73. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

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

75. 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.

76. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to and failing to thwart the Data Breach.

Defendant's Conduct Violates HIPAA.

77. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information (PHI).

78. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

79. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

80. A Data Breach, such as the one Defendant experienced, is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

81. Defendant's Data Breach resulted from a combination of insufficiencies that

demonstrate its failure to comply with safeguards mandated by HIPAA.

Defendant Breached its Obligations to Plaintiff and Class.

82. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its patients' data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident

tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

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

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding data security, as well as PHI, as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

83. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members'

Private Information.

84. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft

85. Data Breaches such as the one Plaintiff and Class Members experienced cause significant disruption to the overall daily lives of victims affected by the attack.

86. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[26] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff and Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

87. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

88. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their

[26] https://www.gao.gov/assets/gao-19-230.pdf (last visited August 14, 2025).

credit reports.[27]

89. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

90. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

91. Theft of Private Information is also gravely serious. PII/PHI is valuable property.[28]

92. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to GAO:

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

See 2007 GAO Report, at p. 29.

93. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

94. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class

---

[27] *See* https://www.identitytheft.gov/Steps (last visited August 14, 2025).

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

Members are at an increased risk of fraud and identity theft for many years into the future. This is evidenced by the fraud that has already taken place in Plaintiff Jane Doe's case, as discussed in further detail below. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

95. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[29]

96. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[30] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[31] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

97. Moreover, it is not an 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. Even then, a new Social Security number may not be effective, as "[t]he

[29] https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last visited August 14, 2025).
[30] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited August 14, 2025).
[31] *Id.* at 4.

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."[32]

98. This data, as one would expect, commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[33]

99. In recent years, the medical and financial industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF'S EXPERIENCES

Plaintiff Jane Doe

100. Plaintiff Jane Doe is and was Defendant's patient at all times relevant to this Complaint. Plaintiff Jane Doe received a Notice of Data Security Incident Letter, related to Defendant's Data Breach, dated July 1, 2025. *See* Exhibit A.

101. In addition, Plaintiff Jane Doe received notice that the Private Information belonging to her minor child, J.L., was among that exfiltrated as part of the Data Breach.

102. The Notice Letters that Plaintiff received do not explain exactly which parts of her

[32] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited August 14, 2025).

[33] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited August 14, 2025).

PII and PHI were accessed and taken but instead generically states that the files contained her name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

103. Plaintiff Jane Doe 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.

104. Since the Data Breach, Plaintiff Jane Doe 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.

105. Soon after the Data Breach, Plaintiff Jane Doe 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.

106. Plaintiff Jane Doe 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.

107. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PII 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.

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

109. 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 and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

110. 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.

111. 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.

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

PLAINTIFF'S AND CLASS MEMBERS' COMMON INJURIES

113. To date, Defendant has done absolutely nothing to compensate Plaintiff and Class Members for the damages they sustained in the Data Breach.

114. Defendant offered only one year of credit monitoring to class members.

115. Defendant fails to offer any compensation to victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiff's and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

116. Furthermore, Defendant's failure to safeguard Plaintiff's and Class Members' Private Information, places the burden squarely on Plaintiff and the Class, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts and omissions resulting in the Data Breach. Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

117. Plaintiff and Class Members have been damaged by the compromise and exfiltration, by cyber-criminals, of their Private Information as a result of the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

118. Plaintiff and Class Members were damaged in that their Private Information is now in the hands of cyber criminals being sold and potentially for sale for years into the future.

119. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft, especially in light of the actual fraudulent misuse of the Private Information that has already taken place, as alleged herein.

120. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

121. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

122. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential

fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

123. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

124. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

125. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing “freezes” and “alerts” with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit

and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

126. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information as well as health information is not accessible online and that access to such data is password-protected.

127. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

128. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach ***since May 2, 2025***and did not notify the victims until July 1, 2025. Yet Defendant offered no explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increased the injuries to Plaintiff and Class.

CLASS ACTION ALLEGATIONS

129. Plaintiff brings all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All persons whose Private Information was compromised as a result of the Data Breach that is the subject of the Notice of Data Security Incident published by Defendant on or about July 1, 2025 (the "Class" or "Class Members").

130. 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.

131. This proposed Class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the Class definition in an amended pleading or when she moves for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

132. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiff is informed and believes, and thereon alleges, that there are at minimum, over a thousand members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Radiology Associates' records, including but not limited to the files implicated in the Data Breach.

133. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Radiology Associates had a duty to protect Plaintiff's and Class members' PII;

b. Whether Radiology Associates was negligent in collecting and storing Plaintiff's and Class members' PII, and breached its duties thereby;

c. Whether Radiology Associates of Richmond, INC. breached its fiduciary duty to Plaintiff and the Class;

d. Whether Radiology Associates breached its duty of confidence to Plaintiff and the Class;

e. Whether Radiology Associates violated its own Privacy Practices;

f. Whether Radiology Associates entered a contract implied in fact with Plaintiff and the Class;

g. Whether Radiology Associates of breached that contract by failing to adequately safeguard Plaintiff's and Class members' PII;

h. Whether Radiology Associates was unjustly enriched;

i. Whether Plaintiff and Class members are entitled to damages as a result of Radiology Associates' wrongful conduct; and

j. Whether Plaintiff and Class members are entitled to restitution as a result of Radiology Associates' wrongful conduct.

134. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class all had information stored in Radiology Associates' system, each having their PII exposed and/or accessed by an unauthorized third party.

135. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex Class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's

counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

136. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

137. **Superiority, Fed. R. Civ. P. 23(b)(3):** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Radiology Associates. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

138. Radiology Associates 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.

139. 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 Radiology Associates failed to timely and adequately notify the

public of the Data Breach;

b. Whether Radiology Associates owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Radiology Associates' security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Radiology Associates' failure to institute adequate protective security measures amounted to negligence;

e. Whether Radiology Associates failed to take commercially reasonable steps to safeguard consumers' and employees' PII; and

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

140. Finally, all members of the proposed Class are readily ascertainable. Radiology Associates has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiff and Class Members)

141. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

142. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare/medical and/or employment.

143. By collecting and storing this data in Defendant's computer network and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer network—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

144. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

145. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

146. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

147. In addition, Defendant had a duty to employ reasonable security measures under

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

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

149. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

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

breaches in the healthcare industry.

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

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

153. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

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

COUNT II
Breach of Contract
(On Behalf of Plaintiff and Class Members)

155. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

156. Plaintiff and Class Members entered into a valid and enforceable contract through which they paid money to Defendant in exchange for services including promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information.

157. Defendant's Privacy Policy memorialized the rights and obligations of Defendant and its patients. This document was provided to Plaintiff and Class Members in a manner in which it became part of the agreement for services.

158. In the Privacy Policy, Defendant commits to protecting the privacy and security of private information and promises to never share Plaintiff's and Class Members' Private

Information except under certain limited circumstances.

159. Plaintiff and Class Members fully performed their obligations under their contracts with Defendant.

160. However, Defendant did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore Defendant breached its contracts with Plaintiff and Class Members.

161. Defendant allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class Members' Private Information without permission. Therefore, Defendant breached the Privacy Policy with Plaintiff and Class Members.

162. Defendant's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in Defendant providing to Plaintiff and Class Members that were of a diminished value.

163. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiff and Class Members.

164. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

165. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiff and Class Members for a period of ten years.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and Class Members)

166. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

167. This Claim is pleaded in the alternative to Count II above.

168. Through their course of conduct, Defendant, Representative Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiff's and Class Members' Private Information.

169. Defendant solicited, invited and required Representative Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Representative Plaintiff and Class Members accepted Defendant's offers by, in part, providing their Private Information to Defendant.

170. As a condition of being direct customers and/or employees of Defendant, Representative Plaintiff and Class Members provided and entrusted their Private Information to Defendant. In so doing, Representative Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiff and Class Members if its data had been breached and compromised or stolen.

171. A meeting of the minds occurred when Representative Plaintiff and Class Members agreed to, and did, provide their Private Information to Defendant, in exchange for, amongst other things, the protection of their Private Information.

172. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

173. Defendant breached the implied contracts it made with Representative Plaintiff and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data Breach.

174. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiff and Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (f) other economic and noneconomic harm.

COUNT IV
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and Class Members)

175. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

176. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

177. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Representative Plaintiff and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the

systems that were exploited in the Data Breach.

178. Defendant acted in bad faith and/or with malicious motive in denying Representative Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, pray for relief as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiff as a Class Representative and her counsel as Class Counsel;

b. For equitable relief enjoining Radiology Associates from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c. For equitable relief compelling Radiology Associates to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Radiology Associates' wrongful conduct;

e. Ordering Radiology Associates to pay for not less than three years of credit monitoring for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and,

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demand a trial by jury on all claims so triable.

Dated: August 18, 2025

Respectfully submitted,

By: */s/ Lee A. Floyd*
Lee A. Floyd (VSB No. 88459)
Justin M. Sheldon (VSB No. 82632)
BREIT BINIAZAN, PC
2100 East Cary Street, Suite 310
Richmond, Virginia 23223
Telephone: (804) 351-9040
Facsimile: (804) 351-9170
Lee@bbtrial.com
Justin@bbtrial.com

Liberato P. Verderame*
Marc H. Edelson*
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
T: (215) 867-2399
medelson@edelson-law.com
lverderame@edelson-law.com

Attorneys for Plaintiff and the Putative Class

* *Pro hac vice forthcoming*