NORTH CAROLINA

IN THE GENERAL COURT OF JUSTICE
SUPERIOR COURT DIVISION

PITT COUNTY

MASTER FILE NO. 24-CVS-772

TAMMY FLYNN, HEISHA LYNCH, J.L., a minor through her mother, HEISHA LYNCH, DEAN SWINSON, BRANDON CANNON, BRITTANY MOORE, ANNAIA McLAMB, CYNTHIA MEADOWS, SUZANNE ABRAMS, LATASHA WILLIAMS, BILLY ROBINSON, JOSEPH SAWYER, SAMANTHA RICHARDSON, LORI POWERS, JASON POWERS, GENEVIEVE JONES, ELAINE QUITTKAT, and MARY SHELDON,

Plaintiffs,

v.

EASTERN RADIOLOGISTS, INC.,

Defendant.

CONSOLIDATED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

NOW COME Plaintiffs, by and through their counsel, and allege as follows:

1. Plaintiffs Tammy Flynn, Heisha Lynch, J.L., a minor through her mother, Heisha Lynch, Dean Swinson, Brandon Cannon, Brittany Moore, Annaia McLamb, Cynthia Meadows, Suzanne Abrams, Latasha Williams, Billy Robinson, Joseph Sawyer, Samatha Richardson, Lori Powers, Jason Powers, Genevieve Jones, Elaine Quittkat, and Mary Sheldon ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this putative class action against Defendant Eastern Radiologists, Inc. ("Defendant") to obtain damages, restitution, and injunctive relief from Defendant. Plaintiffs make the following allegations upon information and belief,

except as to their own actions, the investigation of their counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

2. This class action arises out of the cyberattack and data breach to Defendant's computer network between November 20, 2023 and November 24, 2023, which resulted in the theft of nearly 890,000 individuals' personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information").[1]

3. Defendant was negligent and failed to properly secure, safeguard, encrypt, and/or timely and adequately protect or destroy Plaintiffs' and Class Members' (defined below) Private Information that it had acquired and stored for its business purposes.

4. Defendant is a healthcare organization that provides medical treatment and/or employment to individuals, including Plaintiffs and Class Members. Defendant provides and serves "a total of 17 hospitals, seven outpatient centers and 86 points of care in eastern North Carolina."[2] As a healthcare service provider, Defendant knowingly obtains sensitive Private Information and has a resulting duty to securely maintain such information in confidence.

5. Notwithstanding the above, between November 20, 2023 and November 24, 2023, an unauthorized actor infiltrated Defendant's computer network and stole the Private Information of approximately 886,746 individuals (the "Data Breach").[3]

6. Due to Defendant's negligence and data security failures, which resulted in the Data Breach, cybercriminals were able to target Defendant's computer systems and exfiltrate highly

---

[1] *See* https://radiologybusiness.com/topics/healthcare-management/legal-news/proposed-class-action-lawsuit-accuses-radiology-practice-failing-protect-patient-information (last visited: August 2, 2024).
[2] https://www.easternrad.com/ (last visited: August 2, 2024).
[3] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=8E7AE0C5B87E7D179CDEEC8EFAEDF0F1 (last visited: August 2, 2024).

sensitive Private Information. As a result of this Data Breach, the Private Information of Plaintiffs and Class Members remains in the hands of those cybercriminals and has already been misused for nefarious purposes.

7. According to Defendant's website notice, which has since been removed, upon learning of the Data Breach, Defendant "began [their] investigation with the assistance of a cybersecurity firm, and notified law enforcement."[4] However, despite learning that Plaintiffs' and Class Members' Private Information was stolen in the Data Breach on or about November 20, 2023, Defendant, without explanation, delayed and did not begin sending notices to the victims of the Data Breach (the "Notice of Data Breach Letters") until March 4, 2024.

8. As a direct and proximate result of Defendant's negligence and inadequate data security, and the breach of its duty to safely secure Private Information, Plaintiffs' Private Information was stolen by hackers, posted on the dark web, and exposed to an untold number of unauthorized individuals.

9. Based on the public statements of Defendant to date, a wide variety of Private Information was implicated in the Data Breach including, but not limited to, names, physical addresses, Social Security numbers, phone numbers, dates of birth, health insurance account information, provider taxpayer identification numbers, clinical information (*e.g.*, medical history, diagnoses, treatment, dates of service, and provider names), and exam and/or procedure information.

10. The Data Breach was a direct result of Defendant's negligence and failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect

[4] https://www.easternrad.com/notice-of-security-incident/ (last accessed May 22, 2024).

Plaintiffs' and Class Members' Private Information with which it was entrusted for either treatment or employment or both.

11. Plaintiffs bring this class action lawsuit on behalf of themselves and approximately 890,000 similarly situated persons to address Defendant's negligence and inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their Private Information was stolen.

12. 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 Plaintiffs' 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 property in a dangerous condition.

13. Defendant disregarded Plaintiffs' and Class Members' rights 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 Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and full notice of the Data Breach.

14. 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 intrusion sooner rather than allowing

cybercriminals a period of days of unimpeded access to the Private Information of Plaintiffs and Class Members.

15. Plaintiffs' and Class Members' identities are now exposed because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

16. Armed with the Private Information stolen 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.

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

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

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

20. Accordingly, Plaintiffs and Class Members bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence

per se, (iii) breach of implied contract, (iv) breach of fiduciary duty; (v) unjust enrichment; (vi) invasion of privacy; (vii) breach of the North Carolina Unfair and Deceptive Trade Practices Act; and (viii) declaratory and injunctive relief.

21. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including Defendant's disclosure, expeditiously, of the full nature of the Data Breach and the types of Private Information accessed, obtained, or exposed by the hackers, improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services and identify theft protection services funded by Defendant, and declaratory relief.

PARTIES

22. Plaintiff Tammy Flynn is and at all times mentioned herein was an adult individual and a natural person residing in Pitt County, North Carolina, where she intends to remain.

23. Plaintiff Heisha Lynch is and at all times mentioned herein was an adult individual and natural person residing in Martin County, North Carolina, where she intends to stay.

24. Plaintiff J.L., a minor through her mother, Heisha Lynch, is and at all times mentioned herein was an individual and a natural person residing in Martin County, North Carolina, where she intends to stay.

25. Plaintiff Dean Swinson is and at all times mentioned herein was an adult individual and a natural person residing in Beaufort County, North Carolina, where he intends to stay.

26. Plaintiff Brandon Cannon is and at all times mentioned herein was an adult individual and a natural person residing Pitt County, North Carolina, where he intends to stay.

27. Plaintiff Brittany Moore is and at all times mentioned herein was an adult individual and a natural person residing in Mecklenburg County, North Carolina, where she intends to stay.

28. Plaintiff Annaia McLamb is and at all times mentioned herein was an adult individual and a natural person residing in Edgecombe County, North Carolina, where she intends to stay.

29. Plaintiff Cynthia Meadows is and at all times mentioned herein was an adult individual and a natural person residing in Craven County, North Carolina, where she intends to stay.

30. Plaintiff Suzanne Abrams is and at all times mentioned herein was an adult individual and a natural person residing in Wilson County, North Carolina, where she intends to stay.

31. Plaintiff Latasha Williams is and at all times mentioned herein was an adult individual and a natural person residing in Wilson County, North Carolina, where she intends to stay.

32. Plaintiff Billy Robinson is and at all times mentioned herein was an adult individual and a natural person residing in Edgecombe County, North Carolina, where he intends to stay.

33. Plaintiff Joseph Sawyer is and at all times mentioned herein was an adult individual and a natural person residing in Pamlico County, North Carolina, where he intends to stay.

34. Plaintiff Samantha Richardson is and at all times mentioned herein was an adult individual and a natural person residing in Nash County, North Carolina, where she intends to stay.

35. Plaintiff Lori Powers is and at all times mentioned herein was an adult individual and a natural person residing in Gates County, North Carolina, where she intends to stay.

36. Plaintiff Jason Powers is and at all times mentioned herein was an adult individual and a natural person residing in Gates County North Carolina, where he intends to stay.

37. Plaintiff Genevieve Jones is and at all times mentioned herein was an adult individual and a natural person residing in Greene County, North Carolina, where she intends to stay.

38. Plaintiff Elaine Quittkat is and at all times mentioned herein was an adult individual and a natural person residing in Lenoir County, North Carolina, where she intends to stay.

39. Plaintiff Mary Sheldon is and at all times mentioned herein was an adult individual and a natural person residing in Pitt County, North Carolina, where she intends to stay.

40. Defendant Eastern Radiologists, Inc. is a North Carolina corporation with its principal place of business at 1711 W. 7th Street, Greenville, North Carolina 27834.

JURISDICTION AND VENUE

41. This Court has original jurisdiction over this matter pursuant to N.C.G.S. § 7A-240. Further, this Court has subject matter jurisdiction over this action because the events or omissions giving rise to the claims brought in this Complaint occurred in Pitt County, North Carolina.

42. This Court has personal jurisdiction over Defendant pursuant to N.C.G.S § 1-75.4 because it is a North Carolina domestic corporation, with its primary place of business located in Pitt County.

43. Venue is proper in this County pursuant to N.C.G.S. § 1-77 and 1-82 because it is the county within which Defendant is headquartered and has the most significant contacts. Further, Defendant may be served in Pitt County, and a substantial part of the events or omissions giving rise to the claim arose in Pitt County.

FACTUAL ALLEGATIONS

Defendant's Business

44. Defendant Eastern Radiologists, Inc. was founded in Greenville, North Carolina in or about 1954.[5]

45. Defendant maintains a diagnostic imaging healthcare practice with six locations across eastern North Carolina. Defendant provides diagnosing imaging, women's imaging, interventional radiology and healthcare consulting. Defendant employs more than seventy (70) board certified physicians, serves seventeen hospitals, operates seven outpatient centers, and eighty-six points of care throughout eastern North Carolina.[6]

46. As a condition of receiving medical care services from Defendant, each patient must provide (and Plaintiffs did provide) Defendant with sensitive, personal, and private information, such as their:

- Full names;
- Physical addresses;
- Social Security numbers;
- Phone numbers;
- Dates of birth;
- Health insurance account information;
- Provider taxpayer identification numbers;
- Clinical information (*e.g.*, medical history, diagnoses, treatment, dates of service, and provider names); and

[5] https://www.easternrad.com/history-message/#toc (last accessed August 6, 2024).
[6] https://www.easternrad.com/ (last accessed August 6, 2024).

- Exam and/or procedure information.

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

48. At all relevant times, Defendant knew it was storing sensitive Private Information and that, as a result, its systems would be an attractive target for cybercriminals.

49. Defendant made promises and representations to Plaintiffs and Class Members that the Private Information collected from them as a condition of obtaining medical services at Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

50. Defendant's own Notice of Privacy Practices ("Privacy Policy")[7] makes clear that it understands that its patients' Private Information is personal and recognizes its duty that Defendant is required by law to protect Plaintiffs' and Class Members' Private Information.

51. Defendant's own published privacy policy states that:

- [Defendant] is required by law to maintain the privacy and security of your protected health information.
- [Defendant] will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- [Defendant] must follow the duties and privacy practices described in this notice and give you a copy of it.
- [Defendant] will not use or share your information other than as described here unless you tell us we can in writing.

[7] https://www.easternrad.com/privacy-policy/ (last accessed August 6, 2024).

52. Upon information and belief, Defendant also provides every patient with a HIPAA compliant disclosure form acknowledging its duties under HIPAA and in which it represents that it will protect patients' Private Information.

53. Defendant also knew that a breach of its systems, and exposure of the information stored therein, would at a minimum result in increased risk of identity theft and fraud against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

54. Defendant agreed to and undertook legal duties to maintain the protected health and Private Information entrusted to it by Plaintiffs 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").

55. Yet, through its failure to properly secure the Private Information of Plaintiffs and Class Members, Defendant failed to meet its own promises of patient privacy.

56. Plaintiffs and Class Members provided their Private Information directly 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.

57. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

The Data Breach

58. According to Defendant's website Notice, between November 20, 2023 and November 24, 2023, an unauthorized party accessed Defendant's network and stole documents on its system, which included the Private Information of Plaintiffs and Class Members.

59. Defendant learned of a cyberattack on its computer systems on or about November 24, 2023.

60. Defendant notified the U.S. Department of Health and Human Services ("HHS") of the Data Breach on or about February 29, 2024, listing 886,746 individuals affected.[8]

61. On or about March 4, 2024, months after Defendant learned that the Class Members' Private Information was stolen by cybercriminals, Defendant's patients began receiving their notices of the Data Breach informing them that their Private Information was stolen in the Data Breach.

62. Omitted from the notices was any explanation as to why Defendant failed to timely inform Plaintiffs and Class Members of the Data Breach's occurrence for months after detecting the cyberattack, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

63. This "disclosure" amounts to no real disclosure at all as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

---

[8] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=8E7AE0C5B87E7D179CDEEC8EFAEDF0F1 (last accessed August 6, 2024).

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

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

66. Defendant had duties to safeguard Plaintiffs' and Class Members' Private Information created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiffs and Class Members.

67. Plaintiffs 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

68. It is well known that PII and PHI, especially Social Security numbers, are 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, and their duties to safeguard such information.

69. Individuals place a high value on the privacy of their Private Information. 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.

70. 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, services, 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."[9]

71. Even if stolen Private Information 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.

72. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

---

[9] "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 accessed August 6, 2024).
[10] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) Information Systems Research 254 (June 2007), https://www.guanotronic.com/~serge/papers/weis07.pdf (last accessed August 6, 2024).

73. Individuals, like Plaintiffs and Class Members, are also 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 hackers' purposes.

74. Victims of data breaches face enduring repercussions when their Social Security numbers are stolen and exploited by hackers, as has unfortunately occurred in this case. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

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

76. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

77. In 2023 alone, there were 3,205 data breaches, resulting in 353,027,892 individuals' personal information being compromised.[12] In fact, in the first quarter of 2024, there have been 841 data breaches, resulting in 28,596,892 individuals' personal information being

[11] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed August 6, 2024).
[12] https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last accessed August 6, 2024).

compromised.[13] A total of 124 of those data breaches have been to companies in the healthcare industry and, therefore, Defendant was more than aware and on notice of the risks of failing to properly safeguard Plaintiffs' and Class Members' Private Information.

78. 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.

79. 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." [14] 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."[15]

80. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgments of data security compromises, and despite Defendant's own acknowledgment of its duty to keep PII and PHI private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and the proposed Class from being stolen.

Data Breaches are Rampant in Healthcare

[13] https://www.idtheftcenter.org/publication/itrc-q1-data-breach-analysis/ (last accessed August 6, 2024).
[14] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed August 6, 2024).
[15] *Id.*

81. 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."[16]

82. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[17]

83. 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.

84. According to an article in the HIPAA Journal, 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."[18]

85. 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 monetized."[19]

86. The HIPAA Journal article goes on to explain that patient records, like those stolen in the Data Breach, are "often processed and packaged with other illegally obtained data to create

---

[16] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited May 23, 2024).

[17] *Id.*

[18] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last accessed August 6, 2024).

[19] *Id.*

full record sets (fullz) that contain extensive information on individuals, often in intimate detail. These full record sets are then sold on dark web sites to other criminals who use the data to obtain documentation such as Social Security cards, driver's license numbers, and passports. The documentation 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."[20]

87. 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]

88. Further, as stated above, in the first quarter of 2024, there have been 841 data breaches, resulting in 28,596,892 individuals' personal information being compromised.[22]

89. 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."[23]

90. Based on the value of its patients' Private Information to cybercriminals and cybercriminals' propensity to target healthcare providers, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

91. 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.

---

[20] *Id.*

[21] https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far (last accessed August 6, 2024).

[22] https://www.idtheftcenter.org/publication/itrc-q1-data-breach-analysis/ (last accessed August 6, 2024).

[23] https://www.ahu.edu/blog/data-security-in-healthcare (last accessed August 6, 2024).

Defendant Failed to Comply with FTC Guidelines

92. 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.

93. 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 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]

94. 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.

---

[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 accessed August 6, 2024).
[25] *Id.*

95. The FTC has brought enforcement actions against businesses, like 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.

96. 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.").

97. Defendant failed to properly implement basic data security practices. Defendant had a duty under the FTC Act to implement such basic data security practices. However, Defendant failed to do so.

98. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

99. Defendant was at all times fully aware of its obligation to protect the Private Information 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

100. 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.

101. 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.

102. 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.

103. 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.

104. 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

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

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

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

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

109. 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.

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

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

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

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

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

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

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

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

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

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

Defendant Breached its Obligations to Plaintiffs and Class

111. Defendant breached its obligations to Plaintiffs 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 Plaintiffs' and Class Members' 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 comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

f. Faling to adhere to industry standards for cybersecurity as discussed above;

g. 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);

h. 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);

i. 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);

j. 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);

k. 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);

l. 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);

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

n. 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

o. 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).

112. As the result of maintaining its computer systems in a manner that required security upgrading and, as described above, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

113. Accordingly, as outlined below, Plaintiffs 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

114. Data Breaches, such as the one experienced here by Plaintiffs and Class Members, cause significant disruption to the overall daily lives of victims affected by the attack.

115. The unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

116. The FTC 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 credit reports.[26]

117. 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.

118. 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."

119. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the Private Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs.

120. 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.

---

[26] *See* https://www.identitytheft.gov/Steps (last accessed August 6, 2024).

121. Theft of Private Information is also gravely serious. PII and PHI is valuable property.[27]

122. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[28] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[29]

123. The harm done to children and adolescent victims of data breaches are long-lasting. Children have the potential to lose their identities to cyber criminals. Hackers, through cyberattacks, jump on the opportunity to steal children's PII and PHI. Stealing children's PII and PHI is not only lucrative for hackers, but doing so is hard to detect and prevent. Few people are aware of the problem and the consequences can last decades—"hackers could spen[d] more than a decade preying on a child's credit before the fraud is discovered, and by that time, it is possible that repairs will be difficult to make.[30]

124. According to the "2022 Child Identity Fraud Study" authored by Javelin Strategy

---

[27] *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); *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

[28] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last accessed August 6, 2024).

[29] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last accessed August 6, 2024).

[30] Elise Viebeck, *Why Hackers Want Kids' Personal Information*, (May 23, 2015), https://thehill.com/policy/cybersecurity/242865-why-hackers-want-kids-personal-information/ (last accessed August 6, 2024).

& Research, approximately 915,000 children in the United States were victims of identity fraud in 2021, costing an average of $1,128 for a single household and 16 hours of remediation time.[31]

125. The theft of a child's identity is lucrative to a cyber-criminal because it can remain undetected for years, if not decades. Children are less likely to have credit reports than adults in the first place, which means a cybercriminal could establish an entire credit history long before a child realizes they have been victimized.[32]

126. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. As with income tax returns, 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.

127. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[33]

128. Cybercriminals can post stolen Private Information on the cyber black-market for years following a data breach, thereby making such information publicly available.

---

[31] *See* 1.7 Million U.S. Children Fell victim to Data Breaches, According to Javelin's 2022 Child Identity Fraud Study (October 26, 2022), https://javelinstrategy.com/press-release/17-million-us-children-fell-victim-data-breaches-according-javelins-2022-child (last accessed August 6, 2024).

[32] *See* Why Hacker's Want Kids' Personal Information, *supra* note 23.

[33] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf (last visited August 6, 2024).

129. 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.

130. Multiple Plaintiffs have already received notifications that their Private Information was found on the dark web, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

131. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Defendant is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands 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."

132. 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 $1,000 each."[34]

133. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[35] Such fraud

[34] https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last accessed August 6, 2024).
[35] *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 accessed August 6, 2024).

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.[36] 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.

134. 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 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."[37]

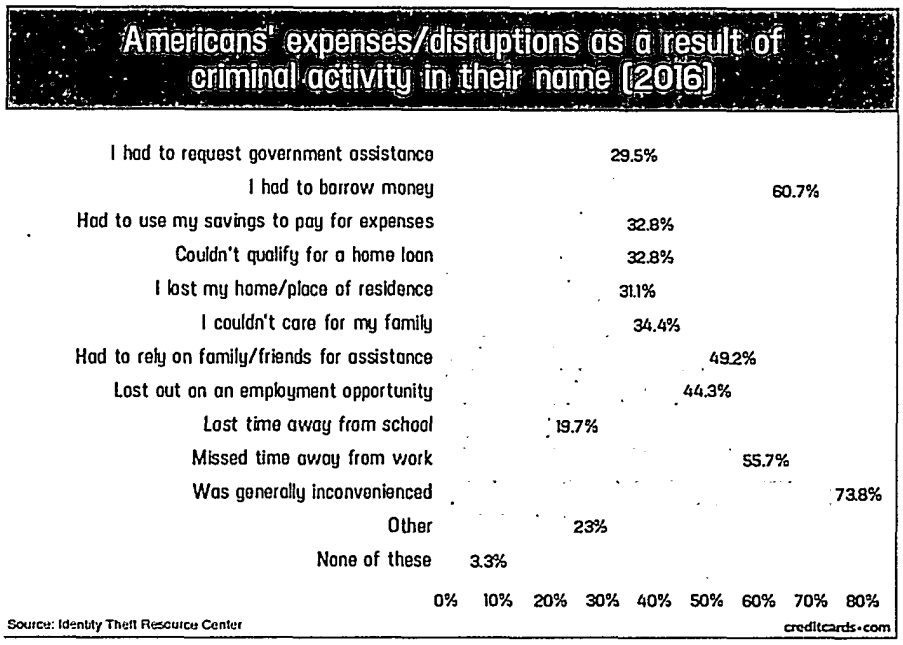
135. It is within this context that Plaintiffs must now live with the knowledge that their Private Information is forever exposed and was stolen by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

136. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.

---

[36] *Id.* at 4.

[37] 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 accessed August 6, 2024).



137. Victims of the Data Breach, like Plaintiffs, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[38]

138. As a direct and proximate result of the Data Breach, and the **theft** of their Private Information, Plaintiffs have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs must now take, and have taken, the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday life, including purchasing identity theft and credit monitoring services every year for the rest of their life, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

[38] *Id.*

139. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training, industry standards, and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' Private Information.

140. Plaintiffs and Class members also have an interest in ensuring that their Private Information that was provided to Defendant is removed from Defendant's unencrypted files.

141. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, Defendant knew or should have known about these dangers and strengthened its data security 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.

PLAINTIFFS' EXPERIENCES

Plaintiff Tammy Flynn's Experience

142. Plaintiff Tammy Flynn is and at all times mentioned herein was an adult individual and a natural person residing in Pitt County, North Carolina, where she intends to remain.

143. Plaintiff provided her information to Defendant as a patient at Eastern Radiologists.

144. Plaintiff Flynn received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

145. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

146. Plaintiff Flynn only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use at least basic security measures to

protect her Private Information, such as requiring passwords and multi-factor authentication to access databases that stored her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

147. Plaintiff Flynn 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.

148. Plaintiff Flynn entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

149. Plaintiff Flynn would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

150. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

151. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

152. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of a significant increase of phishing emails and spam telephone calls, suggesting that her Private

Information is already in the hands of cybercriminals. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

153. The Data Breach has also caused Plaintiff to suffer imminent and impending injury in the form of substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

154. As a result of the actual harm she suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 4-6 hours each month checking her credit reports, monitoring her financial accounts, and sifting through the spam and phishing attempts.

155. In addition, Plaintiff has spent significant time dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was incurred at Defendant's direction.

156. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety, especially the indefinite prospect of her information being available to third parties for the rest of her life.

157. Plaintiff 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.

Plaintiffs Heisha Lynch's and J.L.'s Experiences

158. Plaintiff Heisha Lynch is and at all times mentioned herein was an adult individual and a natural person residing in Martin County, North Carolina, where she intends to stay.

159. Plaintiff J.L. is and at all times mentioned herein was an individual and a natural person residing in Martin County, North Carolina, where he or she intends to stay.

160. Plaintiffs' Private Information was provided to Defendant as patients at Eastern Radiologists.

161. Plaintiff Heisha Lynch received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

162. Plaintiff J.L. received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

163. The notice letter informed Plaintiffs that each of their Private Information was stolen in the Data Breach.

164. Plaintiffs only allowed Defendant to maintain, store, and use their Private Information because they believed that Defendant would use at least basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing their Private Information. As a result, Plaintiffs' Private Information was within the possession and control of Defendant at the time of the Data Breach.

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

166. Plaintiffs entrusted their Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents related to their Private Information.

167. Plaintiffs would not have allowed Defendant to collect and maintain their Private Information had they known that Defendant would not take reasonable steps to safeguard their Private Information.

168. In the instant that their Private Information was accessed and obtained by a third party without their consent or authorization, Plaintiffs suffered injury from a loss of privacy.

169. Plaintiffs have been further injured by the damages to and diminution in value of their Private Information—a form of intangible property that Plaintiffs entrusted to Defendant. This information has inherent value that Plaintiffs was deprived of when their Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

170. Upon information and belief, Plaintiffs' Private Information has already been stolen and misused as they have experienced incidents of fraud and identity theft in the form of a significant increase of spam telephone calls, suggesting that their information is already in the hand of cybercriminals. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiffs' life, specifically by causing financial strain on her as a direct result of the Data Breach.

171. The Data Breach has also caused Plaintiffs to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from their Private Information being placed in the hands of criminals.

172. As a result of the actual harm, they have suffered and the increased imminent risk of future harm, Plaintiff Heisha Lynch has spent approximately 5 hours responding to the Data Breach on behalf of herself and her minor child.

173. The substantial risk of imminent harm and loss of privacy have both caused Plaintiffs to suffer stress, fear, and anxiety, especially the prospect of their information being indefinitely available to third parties for the rest of their lives.

174. Plaintiffs have a continuing interest in ensuring that their Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Dean Swinson's Experience

175. Plaintiff Dean Swinson is and at all times mentioned herein was an adult individual and a natural person residing in Beaufort County, North Carolina, where he intends to stay.

176. Plaintiff provided his information to Defendant as a patient at Eastern Radiologists.

177. Plaintiff Swinson received a notice letter from Defendant Eastern Radiologists in March 2024 informing him of the Data Breach and the exposure of his Private Information.

178. The notice letter informed Plaintiff that his Private Information was stolen in the Data Breach.

179. Plaintiff Swinson only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would at least use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

180. Plaintiff Swinson 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.

181. Plaintiff Swinson entrusted his Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its

agents would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his Private Information.

182. Plaintiff Swinson would not have allowed Defendant to collect and maintain his Private Information had he known that Defendant would not take reasonable steps to safeguard his Private Information.

183. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

184. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

185. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of a significant increase of phishing emails and spam telephone calls. Plaintiff Swinson has also experienced fraudulent activity on his Amazon account in the form of an unauthorized charge, which forced him to dispute the charge with his bank and obtain a new credit card. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and caused him financial strain as a direct result of the Data Breach.

186. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

187. As a result of the actual harm he suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 4-5 hours each week closing his credit card account, checking his credit reports, monitoring his financial accounts, and sifting through the spam and phishing attempts.

188. In addition to the increased risk and the actual harm suffered, the Data Breach has forced Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

189. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety, especially as a business owner.

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

Plaintiff Brandon Cannon's Experience

191. Plaintiff Brandon Cannon is and at all times mentioned herein was an adult individual and a natural person residing Pitt County, North Carolina, where he intends to stay.

192. Plaintiff provided his information to Defendant as a patient at Eastern Radiologists.

193. Plaintiff Cannon received a notice letter from Defendant Eastern Radiologists in March 2024 informing him of the Data Breach and the exposure of his Private Information.

194. The notice letter informed Plaintiff that his Private Information was stolen in the Data Breach.

195. Plaintiff Cannon only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

196. Plaintiff Cannon 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.

197. Plaintiff Cannon entrusted his Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his Private Information.

198. Plaintiff Cannon would not have allowed Defendant to collect and maintain his Private Information had he known that Defendant would not take reasonable steps to safeguard his Private Information.

199. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

200. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

201. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far, as he has received multiple notifications from CreditWise that his name, address, emails and passwords were found on the Dark Web. Further, he was notified by Experian that his address and Social Security number were also found on the Dark Web. Additionally, his credit report reflects incorrect employment history, suggesting fraudulent activity. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and caused him financial strain as a direct result of the Data Breach.

202. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

203. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff spends approximately 30-40 minutes daily, checking his credit reports and financial accounts.

204. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

205. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety, especially as a business owner.

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

Plaintiff Brittany Moore's Experience

207. Plaintiff Brittany Moore is and at all times mentioned herein was an adult individual and a natural person residing in Mecklenburg County, North Carolina, where she intends to stay.

208. Plaintiff provided her information to Defendant when she was a patient at Eastern Radiologists.

209. Plaintiff Moore received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

210. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

211. Plaintiff Moore only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

212. Plaintiff Moore 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.

213. Plaintiff Moore entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that

information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

214. Plaintiff Moore would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

215. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

216. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

217. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of five unauthorized credit inquiries, including but not limited to an inquiry from a Mercedes dealer in Minnesota and an inquiry from Capital One. Following the Data Breach, Plaintiff has experienced an increase in spam calls, suggesting her information is in the hands of cybercriminals. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life, and specifically caused financial strain on her as a direct result of the Data Breach.

218. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

219. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 15 hours checking her credit reports and financial accounts.

220. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

221. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

222. Plaintiff 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 Annaia McLamb's Experience

223. Plaintiff Annaia McLamb is and at all times mentioned herein was an adult individual and a natural person residing in Edgecombe County, North Carolina, where she intends to stay.

224. Plaintiff provided her information to Defendant as a patient at Eastern Radiologists.

225. Plaintiff McLamb received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

226. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

227. Plaintiff McLamb only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

228. Plaintiff McLamb 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.

229. Plaintiff McLamb entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

230. Plaintiff McLamb would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

231. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

232. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

233. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft since the Data Breach. Plaintiff experienced fraud in the form of an unauthorized actor fraudulently taking out student loans in her name; causing her credit score to drop significantly. Plaintiff was unable to apply for a first-time homeowner's program due to this decrease in her credit score. Further, since the Data Beach, Plaintiff has received fraudulent credit card charges and has received multiple bills for medical care she did not receive. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

234. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

235. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 40 hours checking her credit reports, monitoring her financial accounts calling her bank, speaking with attorneys, and dealing with all of the fraudulent charges and activity she has experienced.

236. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to determine if any additional fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

237. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety, especially as a small business owner who has had to devote significant resources to dealing with the breach rather than working on her business ventures.

238. Plaintiff 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 Cynthia Meadows's Experience

239. Plaintiff Cynthia Meadows is and at all times mentioned herein was an adult individual and a natural person residing in Craven County, North Carolina, where she intends to stay.

240. Plaintiff provided her information to Defendant as a patient at Eastern Radiologists.

241. Plaintiff Meadows received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

242. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

243. Plaintiff Meadows only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

244. Plaintiff Meadows 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.

245. Plaintiff Meadows entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

246. Plaintiff Meadows would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

247. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

248. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

249. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud in the form of experiencing a significant increase in spam telephone calls. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and caused financial strain on her as a direct result of the Data Breach.

250. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

251. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 2-3 hours researching the breach, checking her credit reports and financial accounts, and working with lawyers as a result of the Data Breach.

252. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

253. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety, especially the indefinite prospect of her information being available to third parties for the rest of her life.

254. Plaintiff 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 Suzanne Abrams's Experience

255. Plaintiff Suzanne Abrams is and at all times mentioned herein was an adult individual and a natural person residing in Wilson County, North Carolina, where she intends to stay.

256. Plaintiff provided her information to Defendant as a patient at Eastern Radiologists.

257. Plaintiff Abrams received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

258. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

259. Plaintiff Abrams only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

260. Plaintiff Abrams 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.

261. Plaintiff Abrams entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

262. Plaintiff Abrams would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

263. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

264. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

265. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of a significant increase of phishing emails and spam telephone calls, ultimately forcing her to change her telephone number. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and have caused financial strain on her as a direct result of the Data Breach.

266. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

267. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff has spent hours checking her credit reports, monitoring her financial accounts, and sifting through the spam and phishing attempts.

268. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to determine whether fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

269. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety, especially the prospect of her information being available to third parties for the rest of her life.

270. Plaintiff 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 Latasha Williams's Experience

271. Plaintiff Latasha Williams is and at all times mentioned herein was an adult individual and a natural person residing in Wilson County, North Carolina, where she intends to stay.

272. Plaintiff provided her information to Defendant as a patient at Eastern Radiologists.

273. Plaintiff Williams received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

274. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

275. Plaintiff Williams only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would at least use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

276. Plaintiff Williams 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.

277. Plaintiff Williams entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

278. Plaintiff Williams would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

279. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

280. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

281. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft. Plaintiff received notification from Wells Fargo that an unauthorized individual attempted to open an account with her information. Further, Plaintiff has experienced an increase in spam calls following the Data Breach, suggesting that her information is in the hands of cybercriminals. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and caused financial strain on her as a direct result of the Data Breach.

282. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

283. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 5-10 hours checking her credit reports, monitoring her financial accounts, and working with lawyers as a result of the Data Breach.

284. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

285. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety, especially the prospect of her information being indefinitely available to third parties for the rest of her life.

286. Plaintiff 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 Billy Robinson's Experience

287. Plaintiff Billy Robinson is and at all times mentioned herein was an adult individual and a natural person residing in Edgecombe County, North Carolina, where he intends to stay.

288. Plaintiff provided his information to Defendant as a patient at Eastern Radiologists.

289. Plaintiff Robinson received a notice letter from Defendant Eastern Radiologists in March 2024 informing him of the Data Breach and the exposure of his Private Information.

290. The notice letter informed Plaintiff that his Private Information was stolen in the Data Breach.

291. Plaintiff Robinson only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use at least basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to

access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

292. Plaintiff Robinson 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.

293. Plaintiff Robinson entrusted his Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his Private Information.

294. Plaintiff Robinson would not have allowed Defendant to collect and maintain his Private Information had he known that Defendant would not take reasonable steps to safeguard his Private Information.

295. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

296. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

297. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft in the form of a significant increase of phishing text messages and spam telephone calls, often receiving eight to ten calls a

day. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and caused financial strain on him as a direct result of the Data Breach.

298. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

299. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has spent approximately two hours checking his credit reports, monitoring his financial accounts, and speaking with his bank.

300. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

301. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety, especially as a business owner.

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

Plaintiff Joseph Sawyer's Experience

303. Plaintiff Joseph Sawyer is and at all times mentioned herein was an adult individual and a natural person residing in Pamlico County, North Carolina, where he intends to stay.

304. Plaintiff provided his information to Defendant as a patient at Eastern Radiologists.

305. Plaintiff Sawyer received a notice letter from Defendant Eastern Radiologists in March 2024 informing him of the Data Breach and the exposure of his Private Information.

306. The notice letter informed Plaintiff that his Private Information was stolen in the Data Breach.

307. Plaintiff Sawyer only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use at least basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

308. Plaintiff Sawyer 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.

309. Plaintiff Sawyer entrusted his Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his Private Information.

310. Plaintiff Sawyer would not have allowed Defendant to collect and maintain his Private Information had he known that Defendant would not take reasonable steps to safeguard his Private Information.

311. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

312. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This

information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

313. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of multiple unauthorized charges on his debit cards in the months following Data Breach. Each time this occurred, Plaintiff has had to request new cards and spend time resetting information on his various accounts. Plaintiff has also experienced a significant increase in spam telephone calls and text messages following the Data Breach, suggesting that his information is in the hands of cybercriminals. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and caused financial strain on him as a direct result of the Data Breach.

314. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

315. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff spends approximately 15 minutes every day checking his credit reports and financial accounts.

316. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

317. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety, especially of identity theft.

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

Plaintiff Samantha Richardson's Experience

319. Plaintiff Samantha Richardson is and at all times mentioned herein was an adult individual and a natural person residing in Nash County, North Carolina, where she intends to stay.

320. Plaintiff provided her information to Defendant as a patient at Eastern Radiologists.

321. Plaintiff Richardson received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

322. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

323. Plaintiff Richardson only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use at least basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

324. Plaintiff Richardson 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.

325. Plaintiff Richardson entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that

information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

326. Plaintiff Richardson would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

327. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

328. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

329. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of receiving a significant increase in spam text messages and phone calls, specifically about vehicle warranties, suggesting that her Private Information is already in the hands of cybercriminals. Further, following the Data Breach, she has received multiple notices for credit card applications which she did not apply for. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and caused financial strain on her as a direct result of the Data Breach.

330. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

331. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 3-5 hours researching the breach, checking her credit reports, monitoring her financial accounts, and working with lawyers as a result of the breach.

332. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

333. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety, especially the indefinite prospect of her information being available to third parties for the rest of her life.

334. Plaintiff 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 Lori Powers's Experience

335. Plaintiff Lori Powers is and at all times mentioned herein was an adult individual and a natural person residing in Gates County, North Carolina, where she intends to stay.

336. Plaintiff provided her information to Defendant as a patient at Eastern Radiologists.

337. Plaintiff Powers received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

338. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

339. Plaintiff Powers only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use at least basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

340. Plaintiff Powers 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.

341. Plaintiff Powers entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

342. Plaintiff Powers would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

343. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

344. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

345. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft in the form of spam text messages and phone calls, suggesting her information is already in the hands of cybercriminals. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

346. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

347. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 3-4 hours researching the breach, checking her credit reports, monitoring her financial accounts, and working with lawyers as a result of the Data Breach.

348. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

349. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety, especially the indefinite prospect of her information being available to third parties for the rest of her life.

350. Plaintiff 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 Jason Powers's Experience

351. Plaintiff Jason Powers is and at all times mentioned herein was an adult individual and a natural person residing in Gates County North Carolina, where he intends to stay.

352. Plaintiff provided his information to Defendant as a patient at Eastern Radiologists.

353. Plaintiff Powers received a notice letter from Defendant Eastern Radiologists in March 2024 informing him of the Data Breach and the exposure of his Private Information.

354. The notice letter informed Plaintiff that his Private Information was stolen in the Data Breach.

355. Plaintiff Powers only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use at least basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

356. Plaintiff Powers 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.

357. Plaintiff Powers entrusted his Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his Private Information.

358. Plaintiff Powers would not have allowed Defendant to collect and maintain his Private Information had he known that Defendant would not take reasonable steps to safeguard his Private Information.

359. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

360. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

361. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft in the form of spam phone calls and text messages. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and caused financial strain on him as a direct result of the Data Breach.

362. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

363. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 3-4 hours researching the breach, checking his credit reports, changing passwords, monitoring his financial accounts, and working with lawyers as a result of the Data Breach.

364. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring

his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

365. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety, especially the prospect of his information being indefinitely available to third parties for the rest of his life.

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

Plaintiff Genevieve Jones's Experience

367. Plaintiff Genevieve Jones is and at all times mentioned herein was an adult individual and a natural person residing in Greene County, North Carolina, where she intends to remain.

368. Plaintiff provided her information to Defendant as a patient at Eastern Radiologists.

369. Plaintiff Jones received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

370. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

371. Plaintiff Jones only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use at least basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases that stored her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

372. Plaintiff Jones 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.

373. Plaintiff Jones entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

374. Plaintiff Jones would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

375. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

376. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

377. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of a significant increase of phishing text messages and spam telephone calls, suggesting that her Private Information is already in the hands of cybercriminals. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole.

378. The Data Breach has also caused Plaintiff to suffer imminent and impending injury in the form of substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

379. As a result of the actual harm she suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 4 hours each month checking her credit reports, monitoring her financial accounts, and sifting through the spam and phishing attempts.

380. In addition, Plaintiff has spent significant time dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was incurred at Defendant's direction.

381. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety, especially the indefinite prospect of her information being available to third parties for the rest of her life.

382. Plaintiff 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 Elaine Quittkat's Experience

383. Plaintiff Elaine Quittkat is and at all times mentioned herein was an adult individual and a natural person residing in Lenoir County, North Carolina, where she intends to remain.

384. Plaintiff provided her information to Defendant as a patient at Eastern Radiologists.

385. Plaintiff Quittkat received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

386. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

387. Plaintiff Quittkat only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use at least basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases that stored her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

388. Plaintiff Quittkat 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.

389. Plaintiff Quittkat entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

390. Plaintiff Quittkat would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

391. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

392. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was

placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

393. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of a significant increase of phishing text messages, e-mails, and spam telephone calls. Plaintiff Quittkat has also experienced fraudulent activity on one of her credit card accounts in the form of unauthorized charges, which forced her to dispute the charge with her credit card company and obtain a new credit card. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and caused her financial strain as a direct result of the Data Breach.

394. The Data Breach has also caused Plaintiff to suffer imminent and impending injury in the form of substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

395. As a result of the actual harm she suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 8-12 hours each month checking her credit reports, monitoring her financial accounts, and sifting through the spam and phishing attempts. Plaintiff Quittkat has further spent approximately 5 hours having to reset automatic billing for accounts linked to her credit card that she was forced to close due to unauthorized charges.

396. In addition, Plaintiff has spent significant time dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was incurred at Defendant's direction.

397. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety, especially the indefinite prospect of her information being available to third parties for the rest of her life.

398. Plaintiff 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 Mary Sheldon's Experience

399. Plaintiff Mary Sheldon is and at all times mentioned herein was an adult individual and a natural person residing in Pitt County, North Carolina, where she intends to remain.

400. Plaintiff provided her information to Defendant as a patient at Eastern Radiologists.

401. Plaintiff Sheldon received a notice letter from Defendant Eastern Radiologists in March 2024 informing her of the Data Breach and the exposure of her Private Information.

402. The notice letter informed Plaintiff that her Private Information was stolen in the Data Breach.

403. Plaintiff Sheldon only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use at least basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases that stored her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

404. Plaintiff Sheldon 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.

405. Plaintiff Sheldon entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its

agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Private Information.

406. Plaintiff Sheldon would not have allowed Defendant to collect and maintain her Private Information had she known that Defendant would not take reasonable steps to safeguard her Private Information.

407. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

408. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

409. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft. After the Data Breach occurred, Plaintiff Sheldon experienced fraudulent activity by having two credit card accounts opened in her name through no action of her own, which forced her to spend time and effort to close the fraudulent accounts. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole and caused her financial strain as a direct result of the Data Breach.

410. The Data Breach has also caused Plaintiff to suffer imminent and impending injury in the form of substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

411. As a result of the actual harm she suffered and the increased imminent risk of future harm, Plaintiff has spent hours checking her credit reports, monitoring her financial accounts, and sifting through the spam and phishing attempts.

412. In addition, Plaintiff has spent significant time dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was incurred at Defendant's direction.

413. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety, especially the indefinite prospect of her information being available to third parties for the rest of her life.

414. Plaintiff 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

PLAINTIFFS' AND CLASS MEMBERS' INJURIES

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

416. Defendant offered 12-year membership to Experian Identity Works to Class Members, an admission that its failure to protect their Private Information caused Plaintiffs and Class Members long-lasting injuries. The offered services are inadequate when victims are likely to face a lifetime of potential identity theft.

417. Defendant's offer fails to compensate victims of the Data Breach sufficiently for its negligence and unauthorized release and disclosure of Plaintiffs' and Class Members'

Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

418. Furthermore, Defendant's credit monitoring offer and advice to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, 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 Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

419. Defendant fails to compensate 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 Plaintiffs' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

420. Plaintiffs and Class Members have been damaged by the **theft** of their Private Information in the Data Breach, and by the disruption to their lives as a direct and foreseeable consequence of this Data Breach.

421. Plaintiffs and Class Members were damaged in that their Private Information is now in the hands of cyber criminals being sold on the dark web, potentially for years to come.

422. As a direct and proximate result of Defendant's conduct, and the theft of their Private Information, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

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

424. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as fraudulent charges to their accounts, loans attempted to be opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs 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.

425. Plaintiffs and Class Members face a 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 Plaintiffs and Class Members.

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

427. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

428. Plaintiffs 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 financial accounts and 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.

429. Moreover, Plaintiffs 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.

430. Further, as a result of Defendant's conduct, Plaintiffs 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.

431. 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 Private Information. 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 November 24, 2023***, and did not notify the victims until March 4, 2024. In fact, Defendant also admitted that it completed its investigation into the Data Breach on January 26, 2024, but waited until March to begin notifying Plaintiffs and Class Members. Defendant offered no explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increased the injuries to Plaintiffs and Class.

CLASS ACTION ALLEGATIONS

432. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated pursuant to N.C. R. Civ. P. 23.

433. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about March 4, 2024 (the "Class" or "Class Members").

434. Excluded from the Class is Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, members of their immediate families and members of their staff.

435. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification N.C. R. Civ. P. 23

436. Upon information and belief, more than two thirds of the Class Members, as well as the Defendant, are citizens of the State of North Carolina. The principal injuries resulting from the alleged conduct of the Defendant were incurred in the State of North Carolina.

437. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is believed to be 886,746 victims.

438. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. 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;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable federal or state data security laws and regulations, including FTCA and HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant was unjustly enriched as a result of its conduct in connection with the Data Breach;

k. Whether Defendant owed a fiduciary duty to Plaintiffs and Class Members in respect of the information compromised in the Data Breach;

l. Whether Defendant breached a fiduciary duty owed to Plaintiffs and Class Members in respect of the information compromised in the Data Breach;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

439. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised and stolen in the Data Breach. Plaintiff and members of the Class all had information stored in Defendant's system, each of which had their Private Information exposed and/or accessed by an unauthorized third party.

440. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

441. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and acquired in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

442. Superiority. 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

Defendant. 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.

443. 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.

444. Finally, all members of the proposed Class are readily ascertainable. Defendant 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 Plaintiffs and Class Members)

445. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

446. Defendant required Plaintiffs and Class Members to submit non-public Private Information in order to obtain healthcare/medical services, including the Private Information stolen in the Data Breach.

447. By collecting and storing this data in Defendant's computer property, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—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.

448. As discussed below, Defendant's duty was untethered to any contract or other agreement between the Plaintiffs, Class Members, and Defendant, and was a result of Defendant's collection of Plaintiffs' and Class Members' Private Information.

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

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

451. 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, including Social Security numbers, that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

452. Defendant's duty also arose from Defendant's position as a healthcare vendor. Defendant holds itself out as a trusted provider of services for the healthcare industry, and thereby assumes a duty to reasonably protect patients' information. Specifically, 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 Plaintiffs and Class Members from a Data Breach.

453. 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) and (2). 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.

454. 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.

455. 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.

456. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and 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, design, 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. Failing to adequately manage its systems 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;

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

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

f. Failure to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive Private Information;

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

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

i. 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.

457. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and 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.

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

459. 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.

460. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including, but not limited to:

a. Theft of their Private Information;

b. Actual misuse of their Private Information in the form of fraudulent charges to their financial accounts and the posting of their Private Information to the dark web;

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

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

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

f. 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;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

h. 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;

i. Continued risk of exposure to hackers and thieves of their Private Information, 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; and

j. 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.

461. Plaintiffs and Class Members are entitled to damages, including compensatory and consequential damages suffered as a result of the Data Breach, in an amount to be proven at trial.

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

463. Plaintiffs 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
Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

464. Plaintiffs re-allege the above allegations as if fully set forth herein.

465. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

466. 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)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

467. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiffs or Class Members of the Data Breach until March 4, 2024 despite, upon information and belief, Defendant knowing shortly after November 24, 2023 that unauthorized persons had accessed and acquired the Private Information of Plaintiffs and the Class.

468. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

469. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

470. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

471. The harm resulting from the Data Breach was the harm the FTC Act and HIPAA were intended to guard against, and Plaintiffs and Class Members are within the class of persons the statutes were intended to protect.

472. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harm associated with the theft of their Private Information.

473. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs' and Class Members' Private Information was stolen, and they have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

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

474. Plaintiffs re-allege the above allegations as if fully set forth herein.

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

476. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

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

478. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA and the FTC Act, and were consistent with industry standards.

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

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

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

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

483. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

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

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

486. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long-term credit monitoring to all Class Members.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and Class Members)

487. Plaintiffs re-allege the above allegations as if fully set forth herein.

488. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information conveyed to, collected, and maintained by Defendant and that was ultimately stolen in the Data Breach.

489. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' Private Information, and as a healthcare provider, and recipient of patients' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members: (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of the Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store their Private Information.

490. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its current and former patients to keep secure their Private Information.

491. Defendant owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost 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.

492. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect the Private Information collected, diligently discover the Data Breach, investigate the

Data Breach, and give detailed notice of the Data Breach to Plaintiffs and the Class in a reasonable and practicable period of time.

493. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

494. Defendant breached its fiduciary duty owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

495. Defendant breached its fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

496. As a direct and proximate result of Defendant's breaches of its fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, including the increased and imminent risk of future identity theft; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

497. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and Class Members)

498. Plaintiffs re-allege the above allegations as if fully set forth herein. Plaintiffs bring this claim individually and on behalf of all Class Members.

499. This Claim is pleaded in the alternative to Plaintiffs' breach of implied contract and breach of fiduciary duty claims above.

500. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

501. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members are 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.

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

503. 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.

504. 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 security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

505. 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 industry standards.

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

507. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

508. 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.

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

510. As a direct and proximate result of Defendant's breaches of its fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use

of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, including the increased and imminent risk of future identity theft; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

511. 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.

512. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they 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
Invasion of Privacy
(On Behalf of Plaintiffs and Class Members)

513. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

514. Plaintiffs and Class Members had a legitimate expectation of privacy in their Private Information, and were entitled to the protection of this information against disclosure to unauthorized third parties.

515. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

516. Defendant failed to protect such information, and permitted unknown third parties to steal Plaintiffs' and Class Members' Private Information.

517. The unauthorized access and theft of Plaintiffs and Class Members' Private Information is highly offensive to a reasonable person.

518. The Data Breach constituted an intrusion into a place or thing, which is private, and is entitled to be private. Plaintiffs and Class Members disclosed their Private Information to Defendant as part of their use of Defendant's services, but privately, with the intention that their Private Information be kept confidential and be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

520. Defendant acted with a knowing state of mind when it permitted the Data Breach because it had actual knowledge that its information security practices were inadequate and insufficient.

521. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

522. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

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

COUNT VII

Breach of North Carolina's Unfair and Deceptive Trade Practices Act (UDTPA), *N.C. Gen. Stat. § 75-1.1, et. seq.*

(On Behalf of Plaintiffs and Class Members)

524. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

525. It is appropriate to apply North Carolina law to the nationwide class claims because North Carolina's interest in this litigation exceeds that of any other state.

526. Defendant is a North Carolina entity with headquarters in this state and is subject to the laws and regulations of the State of North Carolina, including but not limited to the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. § 75.1.1 ("UDTPA"), which "declare[s] unlawful" all "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." *Id.* § 75-1.1(a).

527. For purposes of North Carolina's UDTPA, the term "commerce" includes all business activities, however denominated, but does not include professional services rendered by a member of a learned profession." *Id.* § 75-1.1(b).

528. Defendant violated the North Carolina UDTPA by engaging in unlawful, unfair, or deceptive business acts and practices in or affecting commerce, as well as unfair, deceptive untrue, or misleading advertising that constitute acts of "unfair competition" prohibited in the statute.

529. Upon information and belief, the policies, practices, acts and omissions giving rise to this action emanated from Defendant's headquarters and facilities in North Carolina.

530. Defendant engaged in unlawful acts and practices with respect to its services by establishing inadequate security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' Private Information with knowledge that such information would not be adequately protected; and by gathering Plaintiffs' and Class Members' sensitive information in an unsecure electronic environment in violation of North Carolina's data

breach statute, the Identity Theft Protection Act, N.C. Gen. Stat. § 75-60, *et seq.*, which requires Defendant to undertake reasonable methods of safeguarding the Private Information of the Plaintiffs and other Class Members.

531. In addition, Defendant engaged in unlawful acts and practices when it failed to discover and then disclose the Data Breach to Plaintiffs and the Class Members in a timely and accurate manner, contrary to the duties imposed by N.C. Gen. Stat. § 75-65.

532. Defendant further violated UDTPA by violating North Carolina's Identity Theft Protection Act (ITPA), N.C. Gen. Stat. § 75-60, *et. seq.* (ITPA) by:

a. Failing to prevent the theft of Plaintiffs' and Class Members' Private Information;

b. Failing to make reasonable efforts to safeguard and protect the Private Information, particularly Social Security numbers, of Plaintiffs and Class Members;

c. Failing to provide adequate notice of the security breach to affected patients upon discovery that its system had been compromised and Private Information had been stolen; and

d. In other ways to be discovered and proven at trial.

533. Defendant willfully concealed, suppressed, omitted and failed to inform Plaintiffs and Class Members of the material facts as described above.

534. Defendant knew or should have known that its data security practices were inadequate to safeguard Plaintiffs' and the Class Members' sensitive information, that the risk of a data security breach was significant, and that its systems were, in fact, breached.

535. Defendant's actions in engaging in the above-named unlawful practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class Members.

536. As a direct and proximate result of Defendant's unlawful acts and practices, Plaintiffs and Class Members have been injured, suffering ascertainable losses and lost money or property, including but not limited to the loss of their legally protected interests in the confidentiality and privacy of their sensitive information.

537. Plaintiffs and the Class Members seek relief under the North Carolina UDTPA including, but not limited to: restitution to Plaintiffs and Class Members of money and property that Defendant has acquired by means of unlawful and unfair business practices; disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices; treble damages (pursuant to N.C. Gen. Stat. § 75-16); declaratory relief; attorneys' fees and costs (pursuant to N.C. Gen. Stat. § 75-16.1); and injunctive or other equitable relief.

COUNT VIII
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiffs and Class Members)

538. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

539. Plaintiff pursues this claim under N.C Gen. St., Chapter 1, Article 26 ("Declaratory Judgments").

540. Defendant owes a duty of care to Plaintiff and the Class that require it to adequately secure Plaintiffs' and the Class's Private Information.

541. Defendant failed to fulfill its duty of care to safeguard Plaintiffs' and Class's Private Information.

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

543. Plaintiff, therefore, seeks a declaration that (1) Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with its explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services and identity theft insurance for Plaintiffs and the Class for a period of ten years; and

h. Meaningfully educating Plaintiffs and the Class about the threats they face as a result of the theft of their Private Information to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a class action under N.C. Gen. Stat. § 1A-1, R. 23, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b) For injunctive relief requiring Defendant to:

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

b. Engage third-party security auditors and internal personnel to run automated security monitoring;

c. Audit, test, and train its security personnel regarding any new or modified procedures;

d. Segment its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conduct regular database scanning and security checks;

f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchase credit monitoring services and identity theft insurance for Plaintiffs and the Class for a period of ten years; and

h. Meaningfully educate Plaintiffs and the Class about the threats they face as a result of the theft of their Private Information to third parties, as well as the steps they must take to protect themselves.

c) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

d) For an award of actual damages, compensatory and/or nominal damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

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

f) Pre- and post-judgment interest on any amounts awarded; and

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

JURY TRIAL DEMANDED

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

Dated: August 20, 2024

Respectfully submitted,

Scott C. Harris
N.C. Bar No.: 35328
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W. Morgan St.
Raleigh, NC 27606
Tel.: (919) 600-5003
Email: sharris@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
Email: gklinger@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877jean
dlietz@milberg.com

Marc H. Edelson*
Shoshana Savett*
EDELSON LECHTZIN LLP
411 South State Street
Suite N-300
Newtown, PA 18940
Tel: (215) 867-2399
medelson@edelson-law.com
ssavett@edelson-law.com

William B. Federman*

Tanner R. Hilton*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081
wbf@federmanlaw.com
trh@federmanlaw.com

Karl S. Gwaltney
N.C. State Bar No. 45118
Edward H. Maginnis
MAGINNIS HOWARD
N.C. State Bar No. 39317
7706 Six Forks Road, Suite 101
Raleigh, North Carolina 27615
Tel: 919-526-0450
Fax: 919-882-8763
kgwaltney@maginnishoward.com
emaginnis@maginnishoward.com

KAPLAN FOX & KILSHEIMER LLP
Laurence D. King, Esq.*
Matthew B. George, Esq.*
Blair E. Reed, Esq.*
Clarissa R. Olivares, Esq.*
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: 415-772-4700
Facsimile: 415-772-4707
lking@kaplanfox.com
mgeorge@kaplanfox.com
breed@kaplanfox.com
colivares@kaplanfox.com

Bryan L. Clobes*
Daniel O. Herrera*
Nickolas J. Hagman*
Mohammed A. Rathur*
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
bclobes@caffertyclobes.com
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

mrathur@caffertyclobes.com

Joel R. Rhine, N.C. State Bar No. 16028
Ruth A. Sheehan, N.C. State Bar No. 48069
RHINE LAW FIRM, P.C.
1612 Military Cutoff Rd., Suite 300
Wilmington, NC 28403
Telephone: (910) 772-9960
jrr@rhinelawfirm.com
ras@rhinelawfirm.com

Jennifer S. Czeisler*
Edward W. Ciolko*
STERLINGTON, PLLC
One World Trade Center
85th Floor
New York, New York 10007
Telephone: (212) 433-2993
jen.czeisler@sterlingtonlaw.com

James M. Evangelista*
EVANGELISTA WORLEY LLC
10 Glenlake Parkway, Suite 130
Atlanta, GA 30328
Tel: (404) 205-8400
Fax: (404) 205-8395
jim@ewlawllc.com

Benjamin F. Johns (PA Bar 201373)*
Samantha E. Holbrook (PA Bar 311829)*
Andrea L. Bonner (PA Bar 332945)*
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Telephone: (610) 477-8380
Fax: (856) 210-9088
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com
abonner@shublawyers.com

David Wilkerson
THE VAN WINKLE LAW FIRM
NCSB 35742
Email: dwilkerson@vwlawfirm.com

11 N Market Street Asheville, NC 28801
Telephone: (828) 258-2991

Daniel Srourian, Esq.*
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: (213)474-3800
Facsimile: (213)471-4160
Email: daniel@slfla.com

Laura Van Note*
COLE & VAN NOTE
55512th St., Suite 2100
Oakland, CA 94607
Telephone: (501) 891-9800
Email: lvn@colevannote.com

F. Hill Allen
N.C. Bar No.: 18884
THARRINGTON SMITH, LLP
P.O. Box 1151
Raleigh, NC 27602
Phone: (919) 821 -4711
Fax: (919) 829-1583
hallen@tharringtonsmith.com

Jean S. Martin*
Francesca K. Burne*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
813-223-5505
jeanmartin@forthepeople.com
fburne@forthepeople.com

Bryan L. Bleichner*
Philip J. Krzeski *
CHESTNUT CAMBRONNE PA
100 Washington A venue South
Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612)-336-2940
bbleichner@chestnutcambronne.com
laukapkrzeski@chestnutcambronne.com

Samuel J. Strauss*
Raina Borrelli*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53 703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Christopher Schehr
NC State Bar No.: 54504
SCHEHR LAW, PLLC
101 N. McDowell St., Unit 200
Charlotte, NC 28204
Tel: 704-900-0036
chris@schehrlaw.com

Attorneys for Plaintiffs and Putative Class
**pro hac vice forthcoming*

CERTIFICATE OF SERVICE

I hereby certify that on August 20, 2024, a true and correct copy of the **CONSOLIDATED CLASS ACTION COMPLAINT** was mailed via FedEx to the Clerk of Court for filing and served on all counsel of record via e-mail listed below

James Davidson
Candice Diah
O'HAGAN MEYER
301 S. McDowell St., Ste. 707
Charlotte, NC 28204
jdavidson@ohaganmeyer.com
cdiah@ohaganmeyer.com

Scott C. Harris