IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE

DANIEL SMITH, RICHARD COHEN, WAYMON BLEVINS, VICKIE LYNN BLEVINS, DANA JONES, individually and on behalf of her minor child A.J., ANN LOVELL, and MATTHEW HAMMOND, on behalf of his minor child R.H., individually and on behalf of all others similarly situated, Plaintiffs, v. SPECIALTY NETWORKS, LLC, and PRIME IMAGING, LLC, Defendants.	Case No. 1:24-cv-00286-CLC-CHS Judge Curtis L. Collier Jury Demand

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Daniel Smith, Richard Cohen, Waymon Blevins, Vickie Lynn Blevins, Dana Jones, individually and on behalf of her minor child A.J., Ann Lovell, and Matthew Hammond, on behalf of his minor child R.H. ("Plaintiffs"), bring this Class Action Complaint against Defendants, Specialty Networks, LLC ("Specialty Networks") and Prime Imaging, LLC ("Prime Imaging") (collectively "Defendants"), individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated current and former patients of Defendants' clients' ("Class Members," defined *infra*) sensitive information, including protected

health information ("PHI") and other personally identifiable information ("PII"), like names, dates of birth, drivers' license numbers, and Social Security Numbers (together with PHI, "Private Information").

2. Based in Chattanooga, Tennessee, Defendant Specialty Networks[1] was founded in 2004 as an application services provider for Picture Archive and Communication Systems (PACS)[2]. Over the course of that first year, Defendants grew to be a provider of radiology information systems (RIS), digital transcription services, and Enterprise Practice Management solutions (EPM) to its clients, which are medical facilities.[3]

3. Defendant Prime Imaging is a radiology medical provider who collected multiple Plaintiffs and many of the proposed Class Members' PII and PHI as a condition them receiving medical treatment.

4. Defendant Prime Imaging is required by HIPAA to ensure that Specialty Networks adheres to the same HIPAA requirements that it is required to implement and maintain, through a business associate agreement.

5. Indeed, if Defendant had properly supervised its service providers, such as Specialty Networks, to ensure it was conveying PII and PHI only to those entities that were compliant with HIPAA, then Plaintiffs' and Class Members sensitive information would not have

[1] Defendants should not be confused with Ohio-based Specialty Networks, which was acquired by Cardinal Health in early 2024. *See* https://radiologybusiness.com/topics/health-it/enterprise-imaging/radiology-information-systems-provider-reports-data-breach.

[2] "[PACS is] a medical imaging technology that provides economical storage, retrieval, management, distribution, and presentation of medical images. PACS storage refers to the storage infrastructure dedicated to housing these medical images and related data within a healthcare facility." https://www.specialtynet.com/about. According to Defendants, "PACS storage plays a crucial role in modern healthcare by facilitating the efficient management and accessibility of medical images, ultimately contributing to improved patient care and outcomes." *Id.*

[3] https://www.linkedin.com/company/specialty-networks-llc/about/.

been exposed to cybercriminals and identity thieves.

6. Defendants received Plaintiffs and Class Members' Private Information in its provision of services to its clients for the benefit of Plaintiffs and Class Members.

7. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

8. On or about August 15, 2024, Defendants announced that an unauthorized actor acquired certain data stored within its systems on or around December 11, 2023, over eight months before the announcement ("Data Breach"). The Private Information of thousands of individuals is believed to have been exposed by the Data Breach.

9. Defendants failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendants' negligent and/or careless acts and omissions and its utter failure to protect its clients' patients' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

10. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised because of Defendants' failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure its network containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal statutes.

11. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

12. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief given that Defendants still maintains custody and control over their Private Information.

13. Plaintiffs and Class Members have suffered injury because of Defendants' conduct, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen because of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

PARTIES

14. Plaintiff Daniel Smith is a resident and citizen of Chattanooga, Tennessee, where he intends to remain.

15. Plaintiff Richard Cohen is a resident and citizen of Cleveland, Tennessee, where he intends to remain.

16. Plaintiff Waymon Blevins is a resident and citizen of South Pittsburg, Tennessee, where he intends to remain.

17. Plaintiff Vickie Lynn Blevins is a resident and citizen of South Pittsburg, Tennessee, where she intends to remain.

18. Plaintiff Dana Jones is a resident and citizen of Chattanooga, Tennessee, where she and her minor child A.J. intend to remain.

19. Plaintiff Ann Lovell is a resident and citizen of Tennessee and is a former patient of Prime Imaging, LLC, who transferred her information to Defendants Specialty Networks.

20. Plaintiff Matthew Hammond is a resident and citizen of Henegar, Alabama, where he and his minor child R.H. intend to remain.

21. Defendant Specialty Networks is a Tennessee limited liability company with its principal place of business located at 1604 Gunbarrel Road, Chattanooga, Tennessee, 37421.

22. Defendant Prime Imaging, LLC is a Georgia limited liability company with its principal place of business in Chattanooga, Tennessee.

JURISDICTION AND VENUE

23. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, there are thousands of Class Members, many of

whom reside outside the state of Tennessee and have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

24. This Court has general personal jurisdiction over Defendants because it is headquartered in this District.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants resides in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendants is subject to the Court's personal jurisdiction with respect to this action.

FACTUAL ALLEGATIONS

Background

26. Plaintiffs provided their Private Information to Specialty Networks, in connection with services they received from their medical providers, such as Prime Imaging.

27. The information held by Defendants in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members, which Defendants should have analyzed to determine which data could have been encrypted or masked.

28. Plaintiffs' and Class Members' Private Information was provided to Defendants with the reasonable expectation and on the understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

29. Indeed, the Private Information disclosed because of Defendants' failures include Plaintiff's protected health information, including their "medical record numbers, treatment and condition information, diagnoses, medications, and health insurance information."[4] And covered entities like Prime Imaging who collect and transfer patient PHI to third parties are required by

[4] Cyber Security Intelligence, *US Healthcare Provider Fails to Protect Customer Data*, (Oct. 1, 2024), https://www.cybersecurityintelligence.com/blog/us-healthcare-provider-fails-to-protect-customer-data-7947.html.

HIPAA to secure business associate agreements with those providers—here, Specialty Networks—to contractually require that they implement reasonable cybersecurity measures.

30. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

31. Defendants had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendants had a legal duty to keep consumer's Private Information safe and confidential.

32. Defendants had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA" or "FTC Act"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

33. Defendants derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendants could not perform the services they provide.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

The Data Breach

35. On August 15, 2024, Specialty Networks announced that an unauthorized actor acquired certain data stored within its systems.

36. The Notice of Data Security Incident sent to Plaintiffs and Class Members states:

> **What Happened?**
> On December 18, 2023, Specialty Networks became aware of unusual activity in our network. Upon discovering this activity, we immediately took steps to secure the network and engaged a digital forensics and incident response firm to conduct an investigation to determine what happened and whether any data within our environment may have been impacted. The investigation revealed that on or about December 11, 2023, an unauthorized actor acquired certain data stored within our stems. Specialty Networks then undertook a comprehensive review of the potentially impacted data and, on May 31, 2024, determined that your personal and/or protected health information may have been involved. We then worked to verify the affected information and mailing addresses for impacted individuals to ensure we had the most up to date contact information…
>
> **What Information Was Involved?**
> Your personal and protected health information that may have been involved in the incident included: name, date of birth, driver's license number, Social Security number, medical record number, treatment and condition information, diagnoses, medications, and health insurance information.[5]

37. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

38. For example, Specialty Networks has admitted that the hackers had infiltrated its systems at least by December 11, 2023, but the malicious activity was not discovered until December 18, 2023. In other words, the hackers were able to infiltrate Specialty Networks' systems, perform reconnaissance functions as is standard practice for hackers, identify the location of files containing Plaintiffs' data, and then exfiltrate that Private Information all without triggering any alarms in Specialty Networks' information systems.

39. These tasks, which are necessary and standard hacker practices, are noisy events

[5] *See* Notice of Data Security Incident provided to Plaintiffs, true and correct copies of which are attached hereto as **Exhibit A**.

that should have been glaringly obvious to Specialty Networks if it had implemented the appropriate logging, monitoring, and centralized alerting tools that are expected in a reasonable cybersecurity program, including endpoint detection and response tools, data loss prevention tools, and centralized alerting systems such as a security information and event management tool.

40. Moreover, given that Defendants discovered the Data Breach on December 18, 2023, but then were incapable of notifying affected individuals in a reasonable and timely manner, it is obvious that Defendants failed to implement and/or test a cybersecurity incident response plan. Indeed, creating such plans and performing regular tabletop exercises to test and improve such plans is a standard part of any reasonable cybersecurity program.

41. Plaintiffs further believe their Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Defendants Collect and Store the Private Information of Plaintiffs and Class Members

42. Specialty Networks derives a substantial economic benefit from providing services to its clients (i.e., Plaintiffs' and Class Members' medical providers such as Prime Imaging), and as a part of providing those services, Specialty Networks retains and stores Plaintiffs' and Class Members' Private Information.

43. Prime Imaging derives a substantial economic benefit from providing services to its patients (i.e. Plaintiffs and Class Members), and as a part of providing medical services, Prime Imaging retains and stores Plaintiffs' and Class Members' Private Information.

44. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known they were responsible for protecting the Private Information from disclosure.

45. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

46. Plaintiffs and Class Members relied on Defendants to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

47. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

48. Upon information and belief, Defendants made promises to Plaintiffs and Class Members to maintain and protect Plaintiffs' and Class Members' Private Information, demonstrating an understanding of the importance of securing Private Information.

49. Defendants' negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

The Data Breach was Imminently Foreseeable

50. Defendants' data security obligations were particularly important given the prevalence of cyberattacks, especially in the healthcare sector.

51. Data thieves regularly target institutions like Defendants due to the highly sensitive information in their custody. Defendants knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

52. The healthcare sector is a particularly common target of data thieves. Indeed, 2024 has seen several high-profile healthcare sector data breaches, including Change Healthcare,

Ascension Health. But this was not new, the healthcare sector has long been targeted.[6]

53. "Healthcare remains a top target for online criminal groups. These data breach costs are the highest of any industry and have increased for the 13th consecutive year."[7]

54. Notwithstanding the foreseeability of the harms caused by these data breaches, "Cybersecurity investment in healthcare tends to lag behind other industries. The healthcare industry reportedly spends 6% to 10% of its overall IT budget on cybersecurity, where the average spend is around 6%."[8]

55. As custodians of Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members because of a breach.

56. In fact, in the first quarter of 2023 alone, "41,452,622 healthcare records were compromised or impermissibly disclosed."[9]

57. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[10] Indeed, during 2019 alone, over 41 million health care records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[11] In short, these sorts of data breaches are

---

[6] Steve Adler, *H1, 2024 Healthcare Data Breach Report*, THE HIPAA JOURNAL (July 30, 2024), https://www.hipaajournal.com/h1-2024-healthcare-data-breach-report.
[7] Michelle Greenlee, *Cost of a Data Breach 2023: Healthcare Industry Impacts*, SECURITY INTELLIGENCE (Aug. 16, 2023), https://securityintelligence.com/articles/cost-of-a-data-breach-2023-healthcare-industry-impacts.
[8] *Id.*
[9] Christine Garcia, *Healthcare Data Breach Report for June 2023*, HIPAA NEWS (Aug. 10, 2023), https://www.calhipaa.com/healthcare-data-breach-report-for-june-2023.
[10] Adil Hussain Seh et el., *Healthcare Data Breaches: Insights and Implications*, NAT'L LIBRARY OF MEDICINE, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636.
[11] Steve Adler, *December 2019 Healthcare Data Breach Report*, The HIPAA JOURNAL (Jan. 21, 2020), https://www.hipaajournal.com/december-2019-healthcare-data-breach-report.

increasingly common, especially among health care systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[12]

58. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

59. Defendants were, or should have been, fully aware of the unique type and significant volume of data in its systems, and the significant number of individuals who would be harmed by the exposure of the unencrypted data, including the more than 400,000 individuals whose Private Information was affected in this Data Breach.

60. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

61. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly PHI—fraudulent use of that information and damage to victims may continue for years.

62. The harms done by these data breaches is just as foreseeable. Some harms are obvious, including the expense of investing in credit monitoring and identity theft protection services after the minimal and insufficient offering from defendants expire. Bank fees and costs to restore credit after fraudulent charges are also common, as are direct financial losses from identity theft schemes and fraudulent withdrawals from bank accounts. Credit scores are damaged by

[12] Rody Quinlan, *Healthcare Security: Ransomware Plays a Prominent Role in COVID-19 Era Breaches* (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.

fraudulent credit inquiries when the malicious actors attempt to take loans out in individuals' names (and often succeed).[13]

63. Beyond these economic harms, however, data breach victims commonly suffer emotional distress. "Data breaches can lead to feelings of constant stress and anxiety, similar to the hypervigilance experienced by individuals with PTSD. The violation of personal information in a data breach can trigger intrusive thoughts and memories, contributing to a heightened sense of vulnerability and fear."[14]

64. Upon hearing that their most sensitive data was allowed to fall into the hands of cybercriminals, consumers "reported feeling 'dizzy with shock.'"[15]

65. Nearly 85% of affected consumers reported "disturbances in their sleep habits, 77% reported increased stress levels, and nearly 64% said they had trouble concentrating. Aches, pains, headaches, and cramps were symptoms for nearly 57%."[16]

66. These are harms long recognized in American courts, even going back to Samuel Warren and Louis Brandeis' famous article The Right to Privacy, which was published in the Harvard Law Review more than 130 years ago.[17]

Value of Personally Identifiable Information and Protected Health Information

67. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18]

---

[13] *See* Ido Kilovaty, *Psychological Data Breach Harms*, 23 N.C. J. OF L. & TECH. 1, 16–18 (2021).
[14] Chisolm Ikezuruora, *Mind Matters: Investigating the Impact of Data Breaches on Mental Health*, PRIVACYEND (Feb. 29, 2024), https://www.privacyend.com/impact-data-breaches-mental-health.
[15] Kilovaty, *supra* note 13.
[16] *Id.*
[17] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[18] 17 C.F.R. § 248.201 (2013).

The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[19]

68. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[20]

69. For example, PII can be sold at a price ranging from $40 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

70. Theft of PHI is also gravely serious: "When another person uses your personal information to get medical services or goods, or to gain financially, that is medical identity theft. The thief may use your identity to see a doctor. He or she may get prescription drugs or to file claims with your insurance company in your name. If the thief's medical treatment or diagnosis mixes with your treatment or diagnosis, your health is at risk."[23]

71. The greater efficiency of electronic health records brings the risk of privacy

---

[19] *Id.*

[20] Anita George, *Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.

[21] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

[22] *In the Dark*, VPNOVERVIEW (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark.

[23] Office of the Attorney General of California, *First Aid for Medical Identity Theft: Tips for Consumers*, https://oag.ca.gov/privacy/facts/medical-privacy/med-id-theft (last visited Oct. 23, 2024).

breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the health care industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

72. According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.[24]

73. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[25]

74. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for health care they did not receive to restore coverage.[26] Almost half of medical identity theft victims lose their health care coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were

[24] *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, NAKED SECURITY (Oct. 3, 2019), https://news.sophos.com/en-us/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals.
[25] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft.
[26] *See* Elinor Mills, *Study: Medical Identity Theft is Costly for Victims,* CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

never able to resolve their identity theft at all.[27]

75. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—PHI, names, and dates of birth—is impossible to "close" and difficult, if not impossible, to change.

76. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[28]

77. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

78. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

---

[27] *Id.; see also* Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN (Mar. 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one.
[28] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.
[29] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

Defendants Failed to Comply with FTC Guidelines

79. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTC Act, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

80. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information 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. 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 into 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.

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

82. The FTC has brought enforcement actions against businesses for failing to

adequately and reasonably protect consumer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

83. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices. Defendants' 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.

84. Defendants were at all times fully aware of their obligation to protect the Private Information of consumers under the FTCA yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendants Failed to Comply with HIPAA Guidelines

85. Defendants are covered entities under HIPAA (45 C.F.R. § 160.102) and are 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.

86. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").

See 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

87. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

88. HIPAA's Privacy 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.

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

90. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

91. HIPAA's Security Rule requires defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

92. HIPAA also requires Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of

electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendants are required under HIPAA to "[i]implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

93. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

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

95. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Pt. 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

96. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

97. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in

the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302–164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.

98. Defendants were at all times fully aware of their HIPAA obligations to protect the Private Information of patients yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendants Failed to Comply with Industry Standards

99. Experts studying cybersecurity routinely identify institutions that store Private Information like Defendants as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

100. Some industry best practices that should be implemented by institutions dealing with sensitive Private Information, like Defendants, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting

which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all these industry best practices.

101. Other best cybersecurity practices that are standard at large institutions that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

102. Indeed, NIST has promulgated specific guidelines that companies that are serious about cybersecurity should implement.

103. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Defendants Breached their Duty to Safeguard Plaintiffs' and Class Members' Private Information

104. In addition to their obligations under federal laws, Defendants owed duties to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

105. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data and failed to audit, monitor, or ensure the integrity of their data security

practices. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to implement reasonable logging, monitoring, and alerting systems sufficient to identify malicious activity in time to empower cybersecurity staff to respond to such alerts;

c. Failing to implement and test a reasonable cybersecurity incident response plan;

d. Failing to adhere to industry standards for cybersecurity as discussed above; and

e. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

106. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems, including its employees' email accounts, which contained unsecured and unencrypted Private Information.

107. Had Defendants remedied the deficiencies in their information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

The Data Breach Increases Victims' Risk of Identity Theft

108. Plaintiffs and Class Members are at a heightened risk of identity theft for years to

come.

109. The unencrypted Private Information of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

110. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

111. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

112. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

113. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Full" packages.[30]

114. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

115. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

116. Because of the recognized risk of identity theft, when a data breach occurs, and an

[30] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

117. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

118. These efforts are even more important when, as here, the nature of the information stolen is particularly susceptible to identity theft.

119. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[31]

120. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended

[31] *See* U.S. Gov't Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

fraud alert that lasts for seven 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.[32]

Plaintiffs' Experiences

Daniel Smith

121. Plaintiff Daniel Smith provided his Private Information to Defendants in connection with medical services he received from his medical provider, Prime Imaging.

122. As a condition of receiving medical care, Plaintiff Smith was required to provide his Private Information to Defendants, including his name, date of birth, driver's license number, Social Security number, medical record number, treatment and condition information, diagnoses, medications, and health insurance information.

123. At the time of the Data Breach, Defendants retained Plaintiff's Private information in its system.

124. Defendants deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for eight months.

125. Plaintiff is very careful about sharing his sensitive Private information. He does not provide his Private Information to anyone unless it is necessary. Plaintiff does not give out his personal contact information. Plaintiff also stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information.

126. Plaintiff received the Notice Letter directly from Defendants on or about August 15, 2024, informing him that his Private Information was improperly accessed and obtained by

[32] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.

unauthorized third parties during the Data Breach, including his name, date of birth, driver's license number, Social Security number, medical record number, treatment and condition information, diagnoses, medications, and health insurance information.

127. Because of the Data Breach and the resulting suspicious activity, Plaintiff Smith made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching and verifying the legitimacy of the Data Breach as well as monitoring his financial account for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time on activities in response to the breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and recreation.

128. Plaintiff Smith suffered actual injury from having his Private Information compromised because of the Data Breach including, but not limited to (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen because of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

129. Because of the Data Breach, Plaintiff Smith suffered anxiety due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his private information for purposes of identity theft and fraud. Plaintiff Smith is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

130. Because of the Data Breach, Plaintiff Smith anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

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

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

Richard Cohen

133. Plaintiff Richard Cohen is unsure how Specialty Networks got his Private Information, including his name, Social Security number, and medical information, but assumes it was provided to Specialty Networks by one of his medical providers. Regardless, in collecting and maintaining Private Information, Specialty Networks implicitly agreed that it will safeguard the data using reasonable means.

134. As a condition of receiving medical care, Plaintiff Cohen was required to provide his Private Information to Specialty Networks, including his name, address, contact information, Social Security number, driver's license number, and other sensitive information.

135. At the time of the Data Breach, Specialty Networks retained Plaintiff Cohen's

Private information in its system.

136. Specialty Networks deprived Plaintiff Cohen of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for eight months.

137. Plaintiff Cohen is a software engineer and is very careful about sharing his sensitive Private information. He does not provide his Private Information to anyone unless it is necessary. Plaintiff does not give out his personal contact information. Plaintiff also stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information.

138. Plaintiff Cohen received the Notice Letter directly from Specialty Networks on or about August 20, 2024, informing him that his Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including his name, date of birth, driver's license number, Social Security number, medical record number, treatment and condition information, diagnoses, medications, and health insurance information.

139. Because of the Data Breach and the resulting suspicious activity, Plaintiff Cohen made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching and verifying the legitimacy of the Data Breach as well as monitoring his financial account for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent roughly four to five hours weekly on activities in response to the breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and recreation.

140. Plaintiff Cohen suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the

bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen because of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

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

142. Because of the Data Breach, Plaintiff Cohen suffered anxiety and overall disappointment due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his private information for purposes of identity theft and

fraud. Plaintiff Cohen is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

143. Because of the Data Breach, Plaintiff Cohen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

144. Because of the Data Breach, Plaintiff Cohen is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

Dana Jones, individually and on behalf of her minor child A.J.

146. Plaintiff Dana Jones is the parent and guardian of her minor daughter, A.J., who is a resident of Chattanooga, Tennessee. On or about August 19, 2024, Plaintiff received a Notice Letter directly from Specialty Networks notifying her that A.J.'s Private Information had been compromised in the Data Breach.

147. Plaintiff Dana Jones provided her Private Information to Defendants in connection with medical services she received from her medical provider, Prime Imaging.

148. Plaintiff Jones provided her daughter, A.J.'s Private information to Defendants in connection with medical services A.J. received at Diagnostic Radiology Consultants, P.A.

149. As a condition of receiving medical care, Plaintiff Jones was required to provide her and her daughter's Private Information to Defendants, including her their names, dates of birth, driver's license number, Social Security numbers, medical record numbers, treatment and condition information, diagnoses, medications, and health insurance information.

150. At the time of the Data Breach, Defendants retained Plaintiff Jones' and A.J.'s

Private information in its system.

151. Defendants deprived Plaintiff Jones of the earliest opportunity to guard herself and her daughter against the Data Breach's effects by failing to notify her about it for eight months.

152. Plaintiff Jones is very careful about sharing her sensitive Private information. She does not provide her Private Information to anyone unless it is necessary. Plaintiff Jones does not give out her personal contact information. Plaintiff Jones also stores any documents containing her Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information.

153. Plaintiff Jones received the Notice Letter directly from Defendants on or about August 19, 2024, informing her that her and her daughter's Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including their names, dates of birth, driver's license number, Social Security numbers, medical record numbers, treatment and condition information, diagnoses, medications, and health insurance information.

154. Because of the Data Breach and the resulting suspicious activity, Plaintiff Jones made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching and verifying the legitimacy of the Data Breach as well as monitoring her financial account for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent 5-6 hours a day on activities in response to the breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and recreation.

155. Plaintiff Jones suffered actual injury from having her Private Information compromised because of the Data Breach including, but not limited to (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost

opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen because of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

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

157. Plaintiff Jones is a military veteran who has been diagnosed with an anxiety disorder. She is being treated for it by a doctor at the VA. The Data Breach has increased her anxiety significantly and her doctor prescribed new medications and increased the dosage to help her manage her anxiety due to the Data Breach.

158. Because of the Data Breach, Plaintiff Jones suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her private information for purposes of identity theft and fraud. Plaintiff Jones is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

159. Because of the Data Breach, Plaintiff Jones anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

160. Because of the Data Breach, Plaintiff Jones is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

161. Plaintiff Jones has a continuing interest in ensuring that her Private Information, which remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Matthew Hammond, on behalf of his minor child R.H.

162. Plaintiff Matthew Hammond provided R.H.'s Private Information to Specialty Networks in connection with medical services R.H. received from his medical provider.

163. As a condition of receiving medical care, Plaintiff Hammond was required to provide R.H.'s Private Information to Specialty Networks, including their name, dates of birth, Social Security number, medical record number, treatment and condition information, diagnoses, medications, and health insurance information.

164. At the time of the Data Breach, Defendants retained the same Private information in its information systems.

165. Specialty Networks deprived Plaintiff Hammond of the earliest opportunity to

guard his son against the Data Breach's effects by failing to notify him about it for over eight months.

166. Plaintiff Hammond is very careful about sharing sensitive Private information. He does not provide his Private Information to anyone unless it is necessary. Plaintiff Hammond does not give out his personal contact information. Plaintiff Hammond also stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information.

167. Plaintiff Hammond received the Notice Letter directly from Specialty Networks on or about August 15, 2024, informing him that his son's Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including his name, date of birth, driver's license number, Social Security number, medical record number, treatment and condition information, diagnoses, medications, and health insurance information.

168. Because of the Data Breach and the resulting suspicious activity, Plaintiff Hammond made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching and verifying the legitimacy of the Data Breach as well as monitoring his financial account for any indication of fraudulent activity, which may take years to detect. Plaintiff Hammond has spent significant time on activities in response to the breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and recreation.

169. Plaintiff Hammond suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the

bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen because of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

170. Because of the Data Breach, Plaintiff Hammond suffered anxiety due to the public dissemination of his son's personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his private information for purposes of identity theft and fraud. Plaintiff Hammond is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff Hammond is extremely concerned about his son's Private Information being exposed, especially since his son is so young. It is difficult for Plaintiff Hammond to tell whether his son has experienced fraud because R.H. is a minor and does not have any accounts.

171. Because of the Data Breach, Plaintiff Hammond anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

172. Because of the Data Breach, R.H. is at a present risk and will continue to be at

increased risk of identity theft and fraud for years to come.

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

Waymon and Vickie Lynn Blevins

174. Plaintiffs Waymon and Vickie Blevins provided their Private Information to Specialty Networks in connection with medical services they received from their medical provider.

175. At the time of the Data Breach, Defendant retained Plaintiffs' Private Information in its system.

176. Plaintiffs' Private Information was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Specialty Networks' information systems for the specific purpose of targeting the Private Information.

177. Plaintiffs takes reasonable measures to protect their Private Information. They have never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

178. Because of the Data Breach, Plaintiffs have suffered a loss of time and have spent and continues to spend a considerable amount of time on issues related to this Data Breach. They monitor accounts and credit scores and have sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

179. Plaintiffs suffered lost time, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of their privacy. For one thing, they have noticed a spike in spam and scam calls and emails since the Data Breach.

180. Plaintiffs have suffered imminent and impending injury arising from the

substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information, especially their name and PHI, being placed in the hands of criminals.

181. Defendant obtained and continues to maintain Plaintiffs' Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiffs' Private Information was compromised and disclosed because of the Data Breach.

182. Because of the Data Breach, Plaintiffs anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Because the Data Breach, Plaintiffs is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come, especially considering the nature of the PII affected.

Ann Lovell

183. Plaintiff Ann Lovell is a former patient of Prime Imaging, who collected her Private Information as a condition of receiving such services and then conveyed her information to Defendant Specialty Networks.

184. Prime Imaging utilized Specialty Networks for radiology information systems, digital transcription services, and Enterprise Practice Management solutions.

185. As a condition of receiving Prime Imaging's medical services, Plaintiff was required to provide her Personal Information to Prime Imaging, which Prime Imaging then provided to Specialty Networks in connection with Specialty Networks' radiology software services, including but not limited to Plaintiff's name, date of birth, driver's license number, Social Security number, medical record number, treatment and condition information, diagnoses, medications, and health insurance information.

186. Plaintiff typically takes measures to protect her Personal Information and is very

careful about sharing her Personal Information. Plaintiff has never knowingly transmitted Personal Information over the internet or other unsecured source.

187. Plaintiff stores any documents containing her Personal Information in a safe and secure location, and she diligently chooses unique usernames for her passwords and online accounts.

188. In entrusting her Personal Information to Defendants, Plaintiff believed that, as part of the payments for medical treatment and services, Defendants Prime Imaging and Specialty Networks would adequately safeguard that information. Had Plaintiff known that Prime Imaging did not utilize reasonable data security measures, and that Prime Imaging did not ensure Specialty Networks utilized reasonable data security measures, Plaintiff would not have entrusted her Personal Information to said Defendants or would have paid less for those treatments and services.

189. Plaintiff received Specialty Networks' Notice of Data Security Incident dated August 15, 2024, informing her that her Personal Information, including her name, date of birth, driver's license number, Social Security number, medical record number, treatment and condition information, diagnoses, medications, and health insurance information, was impacted and exfiltrated in the Data Breach.

190. As a direct and proximate result of the Data Breach permitted to occur by Defendants, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Personal Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be used for criminal, fraudulent purposes and/or has been sold for such purposes and posted on the dark web for sale; Plaintiff has been and will be forced to expend considerable time and effort to monitor her accounts and credit files, changing her online account passwords, verifying the legitimacy of Defendant's

Notice of Data Security Incident and researching the Data Breach, to protect herself from identity theft and fraudulent misuse of her Personal Information, disclosed as a result of the Data Breach.

191. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of her Personal Information in the Data Breach.

192. She fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Personal Information. She is experiencing feelings of anxiety, embarrassment, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

193. Plaintiff was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive Personal Information and the harm caused by the Data Breach. She was also outraged that Defendants took months to notify her of the Data Breach even as it was discovered in December 2023.

194. Because of the Data Breach, Plaintiff faces a lifetime risk of identity theft, as it includes PII that cannot be changed (e.g., Social Security number and date of birth).

195. Indeed, Ms. Lovell has already started to see the increased risk of harm come to fruition. She had fraudulent transactions on her bank account, and although those charges were reimbursed, it required that she spend her time setting things straight by calling her bank, seeking reimbursement, ordering a new debit card, and then updating payment information.

196. Furthermore, Plaintiff's sensitive Personal Information remains in Defendants' possession without adequate protection against known threats, exposing Plaintiff to the prospect of additional harm.

CLASS ALLEGATIONS

197. Pursuant to Federal Rules of Civil Procedure 12(b)(2), 23(b)(3), and 23(c)(4), Plaintiffs brings this action on behalf of himself and on behalf of all members of the proposed class defined as:

> All individuals residing in the United States whose Private Information was compromised in the Data Breach ("Class").

198. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

199. Plaintiffs reserve the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

200. The proposed Class meets the criteria certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

201. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believes the proposed Class includes hundreds of thousands of individuals who have been damaged by Defendants' conduct as alleged herein. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendants' records.

202. 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 Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the FTCA;

c. When Defendants learned of the Data Breach;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendants' data security systems, prior to and during the Data Breach, were consistent with industry standards;

g. Whether Defendants owed duties to Class Members to safeguard their Private Information;

h. Whether Defendants breached their duties to Class Members to safeguard their Private Information;

i. Whether hackers obtained Class Members' Private Information via the Data Breach;

j. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

k. Whether Defendants breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

l. Whether Defendants knew or should have known its data security systems and monitoring processes were deficient;

m. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;

n. Whether Defendants' conduct was negligent;

o. Whether Defendants breached contracts it had with its clients, which were made expressly for the benefit of Plaintiffs and Class Members;

p. Whether Defendants were unjustly enriched;

q. Whether Plaintiffs and Class Members are entitled to damages;

r. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

203. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendants. Plaintiffs is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

205. Predominance. Defendants has engaged in a common course of conduct toward Plaintiffs and Class Members. For example, all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The

common issues arising from Defendants' 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.

206. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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 Defendants. In contrast, conducting 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.

207. Class certification is also appropriate under Federal Rule of Civil Procedure 23(b)(2). Defendants has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

208. Finally, all members of the proposed Class are readily ascertainable. Defendants has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

CLAIMS FOR RELIEF

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

209. Plaintiffs incorporate the above allegations as if fully set forth herein.

210. Plaintiffs and Class Members provided their non-public Private Information to Defendants in connection with and as a condition of obtaining medical services from Defendants' clients.

211. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

212. By assuming the responsibility to collect and store this data, Defendants had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

213. Defendants had duties to employ reasonable security measures under Section 5 of the FTCA, 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.

214. Defendants' duty to use reasonable security measures under HIPAA required Defendants 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 the health care and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

215. Defendants 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 their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

216. Moreover, Defendants had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

217. Defendants had and continues to have duties to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

218. Defendants breached its duties, pursuant to the FTCA, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

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

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

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

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

e. Failing to remove Plaintiffs' and Class Members' Private Information it was

no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

219. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

220. Defendants' violation of federal statutes also constitutes negligence *per se*. Specifically, as described herein, Defendants has violated the FTCA and HIPAA.

221. Plaintiffs and Class Members were within the class of persons the FTCA and HIPPA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

222. Defendants has admitted that the Private Information of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

223. But for Defendants' wrongful and negligent breaches of duties owed to Plaintiffs and Class Members, the Private Information of Plaintiffs and Class Members would not have been compromised.

224. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing,

and maintaining appropriate security measures.

225. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen because of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

226. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

227. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate

measures to protect the Private Information in its continued possession.

228. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

COUNT II
Breach of Third Party Beneficiary Contract
Against Specialty Networks
(On Behalf of Plaintiffs and the Class)

229. Plaintiffs incorporate the above allegations as if fully set forth herein.

230. Upon information and belief, Defendants entered into virtually identical contracts with its clients to provide services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

231. Such contracts were made expressly for the benefit of Plaintiffs and Class Members, as it was their Private Information that Defendants agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

232. Defendants knew that if it were to breach these contracts with its clients, Plaintiffs and the Class would be harmed.

233. Defendants breached its contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when Defendants failed to use reasonable data security measures that could have prevented the Data Breach.

234. As foreseen, Plaintiffs and the Class were harmed by Defendants' failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their Private

Information.

235. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen because of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

236. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

237. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

238. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants 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 credit monitoring to all Class Members.

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

239. Plaintiffs incorporate the above allegations as if fully set forth herein.

240. Plaintiffs bring this claim in the alternative to his breach of third-party beneficiary contract claim above.

241. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their Private Information. In exchange, Defendants should have provided adequate data security for Plaintiffs and Class Members.

242. Defendants knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as a necessary part of their receiving services from Defendants' clients. Defendants appreciated and accepted that benefit. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

243. Upon information and belief, Defendants funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

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

245. Defendants, however, failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

246. Defendants would not be able to carry out an essential function of its regular

business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendants or anyone in Defendants' position would use a portion of that revenue to fund adequate data security practices.

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

248. If Plaintiffs and Class Members knew that Defendants had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendants.

249. Defendants 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 Data Breach, Defendants instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize its own profits over the requisite security and the safety of their Private Information.

250. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

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

252. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class

Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen because of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

253. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

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

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

255. Plaintiffs incorporate the above allegations as if fully set forth herein.

256. The exposure of Plaintiffs' and Class Members PII and PHI is objectively and

highly offensive to any reasonable person, especially because the information includes health information and PII that cannot reasonably be changed, such as Social Security numbers and dates of birth, but are directly used to commit identity theft and fraud.

257. The Data Breach represents both an intrusion upon seclusion and a public disclosure of private information.

258. The Data Breach intruded upon Plaintiffs' right to autonomy and control over the decision of who has access to their Private Information.

259. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its communications platforms and services therein.

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

261. Defendants failed to protect said Private Information and exposed it to unauthorized actors.

262. Defendants allowed unauthorized third parties access to and examination of the Private Information of Plaintiffs and the Class Members, by way of Defendants' failure to protect the Sensitive Information.

263. The unauthorized release to, custody of, and examination by unauthorized third parties of the Sensitive Information of Plaintiffs and the Class Members is highly offensive to a reasonable person.

264. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class Members Private Information was disclosed to Defendants as a condition of receiving services, but privately with an intention that the Private Information would

be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

265. The Data Breach constitutes an intentional or reckless interference by Defendants with Plaintiffs' and the Class Members' interests 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.

266. Defendants acted with a knowing state of mind when it permitted the Data Breach to occur because they had actual knowledge that its information security practices were inadequate and insufficient. Indeed, at a minimum, Defendants acted with substantial certainty that their failure to reasonable protect Plaintiffs' Private Information would lead to its disclosure to unauthorized actors.

267. Defendants acted with reckless disregard for Plaintiff's and Class Members' privacy when they allowed improper access to its systems containing Plaintiffs' and Class Members' Privates Information.

268. Defendants were aware of the potential of a data breach and failed to adequately safeguard their systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' Private Information.

269. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class Members.

270. Defendants' disclosure of Plaintiffs' and Class Members' Private Information was also a publication in that the disclosure was made to thousands of identity thieves and

cybercriminals, who are in a special relationship with Plaintiffs the Class Members in that those individuals are precisely the group that foreseeably are intent on misusing Plaintiffs' and Class Members' Private Information. Indeed, the individuals to whom the data was exposed are precisely the individuals that the required cybersecurity measures were intended to protect Plaintiffs and Class Members from, which Defendants know.

271. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class Members in that the Sensitive Information maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class Members.

COUNT V
BREACH OF IMPLIED CONTRACT
Against Prime Imaging, LLC
(On Behalf of Plaintiffs and the Class)

272. Plaintiffs incorporate the above allegations as if fully set forth herein.

273. Plaintiffs and the proposed Class Members transferred their Private Information to Prime Imaging as a condition of receiving health services.

274. Plaintiffs and Class Members conferred a monetary benefit on Prime Imaging. Specifically, they provided it with their Private Information. In exchange, Prime Imaging should have provided adequate data security for Plaintiffs and Class Members and implicitly agreed to.

275. Indeed, Prime Imaging held itself out as a company dedicated to protecting the privacy of Plaintiff's and the proposed Class Members' Private Information.

276. Prime Imaging knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as a necessary part of receiving health services.

277. Prime Imaging, however, failed to secure Plaintiffs and Class Members' Private Information, and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

278. If Plaintiffs and Class Members knew that Prime Imaging had not reasonably secured their Private Information, they would not have allowed it to be provided to Prime Imaging.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiffs, on behalf of himself and Class Members, requests judgment against Defendants and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and his counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

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

   i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

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

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised,

hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and securing checks;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

E. For an award of attorneys' fees and costs, and any other expenses, 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.

DEMAND FOR JURY TRIAL

Plaintiffs demands a trial by jury on all issues so triable.

Dated: November 7, 2024

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (TN BPR # 23045)
Grayson Wells (TN BPR # 039658)
STRANCH, JENNINGS & GARVEY, PLLC

223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Interim Lead Counsel

Lynn A. Toops
Amina A. Thomas
COHEN & MALAD LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

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

Andrew J. Shamis
SHAMIS & GENTILE P.A.
14 NE 1st Avenue, Suite 705
Miami, FL 33132
Tel: (305) 479-2299
ashamis@shamisgentile.com

Jeff Ostrow
Kristen Lake Cardoso
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com
cardoso@kolawyers.com

Samual J. Strauss
Raina Borrelli
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611

Tel: (872) 263-1100
sam@straussborrelli.com
raina@straussborrelli.com

Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on November 7, 2024, a true and correct copy of the foregoing document has been served upon all counsel of record via CM/ECF.

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV