IN THE UNITED STATES DISTRICT COURT OF MISSOURI
WESTERN DISTRICT OF MISSOURI

T.R., D.S., T.S., Breanna Highfill, Charles Leap, Rachel Taylor, Travis Taylor, K.H., H.F., David Dempsey, C.C. on behalf of minor child A.C., Joshua Sartin, and Maria Dunn, individually and on behalf of all others similarly situated, Plaintiffs, v. CLAY-PLATTE FAMILY MEDICINE, P.C. Serve at: Nathan D. Granger, M.D. 5501 NW 62nd Terrace Ste 100 Kansas City, MO 64151 and NATHAN D. GRANGER d/b/a SUMMIT FAMILY AND SPORTS MEDICINE Serve at: Registered Agents Inc. 117 S Lexington St Ste 100 Harrisonville, MO 64701 and COBBLESTONE FAMILY MEDICINE CLINIC d/b/a CLAY PLATTE FAMILY MEDICINE CLINIC, P.C. Serve at: Registered Agents Inc. 117 S Lexington St Ste 100 Harrisonville, MO 64701 and BARRY POINTE FAMILY CARE, LLC	)	Case No: 4:24-cv-00704-SRB

d/b/a BARRY POINTE FAMILY CARE P.C.
Serve at:
Brose, Amy Elaine
9151 NE 81st Terrace Suite
Kansas City, MO 64158

Defendants.

PLAINTIFFS' FIRST AMENDED COMPLAINT

COMES NOW T.R., D.S., T.S., Breanna Highfill, Charles Leap, Rachel Taylor, Travis Taylor, K.H., H.F., David Dempsey, C.C. on behalf of minor child A.C., Joshua Sartin, and Maria Dunn ("Plaintiffs"), individually and on behalf of all citizens who are similarly situated for their First Amended Class Action Complaint for Damages against Defendants Clay-Platte Family Medicine, P.C., Nathan D. Granger d/b/a Summit Family and Sports Medicine, Cobblestone Family Medicine Clinic d/b/a Clay Platte Family Medicine Clinic P.C., and Barry Pointe Family Care, LLC d/b/a Barry Pointe Family Care (collectively "Defendants" or "the Clinics") and respectfully states and alleges as follows:

NATURE OF THE CASE

1. This is a class action brought by Plaintiffs, individually and on behalf of all citizens who are similarly situated (*i.e.*, the Class Members), seeking to redress Defendants' willful and reckless violations of their privacy rights. Plaintiffs and the other Class Members are patients of the Clinics, each of which are Missouri healthcare providers, who entrusted their Protected Health Information ("PHI") and Personally Identifiable Information ("PII") to Defendants (collectively, "Private Information").

2. Defendants were entrusted to protect and keep Plaintiffs' and the Class Members' PHI and PII from wrongful disclosure.

3. This action pertains to Defendants' unauthorized disclosure of the Plaintiffs' PHI and PII that occurred on or around June 26, 2024 (the "Breach").

4. On or about June 26, 2024, an unauthorized third party or person, accessed and downloaded Plaintiffs' and the Class Members' PHI and PII. Each Defendants has independent, non-delegable duties to their patients to safeguard their PHI and PII and are responsible for the wrongful disclosure of Plaintiffs' and the Class Members' PHI and PII.

5. As evidenced by the Data Breach's occurrence, the Private Information contained in Defendants' network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

6. Defendants disclosed Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons as a direct and/or proximate result of Defendants' failure to safeguard and protect their PHI and PII.

7. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiffs' and the other Class Members' name, Social Security Number, physical address, date of birth, medical information, gender, and phone numbers.

8. Defendants flagrantly disregarded Plaintiffs' and the other Class Members' privacy and property rights by intentionally, willfully and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiffs' and the other Class Members' PHI and PII from unauthorized disclosure. Plaintiffs' and the other Class Members' PHI and PII was improperly handled, inadequately protected, readily able to be

copied by anyone with nefarious intent and not kept in accordance with basic security protocols. Defendants' obtaining of the information and sharing of same also represent a flagrant disregard of Plaintiffs' and the other Class Members' rights, both as to privacy and property.

9. Plaintiffs and the other Class Members have standing to bring this action because as a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiffs and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) identity theft, (iii) medical and pharmaceutical fraud, (iv) loss of medical expenses, and/or (v) the additional damages set forth in detail below, which are incorporated herein by reference.

10. Defendants' wrongful actions and/or inaction and the resulting Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft, identity fraud and medical fraud. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report ("the Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PHI and PII is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiffs' and the other Class Members' PHI and PII and not yet used the information will do so at a later date or re-sell it.

11. Plaintiffs and the Class members have also suffered and are entitled to damages for the lost benefit of their bargain with Defendants. Plaintiffs and members of the Class paid Defendants for its services including the protection of their PHI and PII. The lost benefit of the bargain is measured by the difference between the value of what Plaintiffs and the members of the Class should have received when they paid for their services, and the value of what they actually did receive; services without adequate privacy safeguards. Plaintiffs and the members of the Class have been harmed in that they (1) paid more for privacy and confidentiality than they otherwise would have, and (2) paid for privacy protections they did not receive. In that respect, Plaintiffs and the members of the Class have not received the benefit of the bargain and have suffered an ascertainable loss.

12. Additionally, because of Defendants' conduct, Plaintiffs and members of the Classes have been harmed in that Defendants has breached its common law fiduciary duty of confidentiality owed to Plaintiffs and member of the Classes.

13. Accordingly, Plaintiffs and the other Classes seek redress against Defendants for breach of implied contract, outrageous conduct, common law negligence, invasion of privacy of public disclosure of private facts, negligent training and supervision, negligence *per se*, and breach of fiduciary duty of confidentiality.

14. Plaintiffs, individually and on behalf of the other Classes, seeks all (i) actual damages, economic damages, and/or nominal damages, (ii) injunctive relief, and (iii) attorneys' fees, litigation expenses, and costs.

JURISDICTION AND VENUE

15. The Court has jurisdiction over the parties and the subject matter of this action. Jurisdiction is proper because Defendants is a business operating nationwide whose principal place of business is in the state of Missouri.

16. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and at least one Plaintiff and members of the Classes are citizens of states that differ from at least one Defendant.

17. Venue is proper in the Eastern District of Missouri, pursuant to 28 U.S. Code § 1391 because the acts complained of occurred and Defendants are located in this District.

PARTIES

18. Plaintiff T.R. is an adult residing in Daytona Beach, Florida.

19. Plaintiff D.S. is an adult residing in Kanas City, Jackson County, Missouri.

20. Plaintiff T.S. is an adult residing in Kansas City, Missouri.

21. Breanna Highfill is an adult residing in Kansas City, Missouri.

22. Charles Leap is an adult residing in Kansas City, Missouri.

23. Rachel Taylor is an adult residing in Kansas City, Missouri.

24. Travis Taylor is an adult residing in Kansas City, Missouri.

25. K.H. is an adult residing in Kansas City, Missouri.

26. H.F. is an adult residing in Kansas City, Missouri.

27. David Dempsey is an adult residing in Kansas City, Missouri.

28. C.C. is an adult pursuing this action on behalf of his minor child A.C. Both are residents of Lee's Summit, Missouri.

29. Joshua Sartin is an adult residing in Raytown, Missouri.

30. Maria Dunn is an adult residing in Kansas City, Missouri.

31. Defendant Clay-Platte Family Medicine, P.C., is, upon information and belief, a Missouri Corporation with its headquarters in Kansas City, Missouri. Defendant can be served at its Registered Address at 5501 NW 62nd Terrace, Ste. 100, Kansas City, MO 64151.

32. Defendant Nathan D. Granger d/b/a Summit Family and Sports Medicine is, upon information and belief, a Missouri Corporation with its headquarters in Lee's Summit, Missouri. Defendant can be served at its Registered Address at 117 S Lexington St., Ste. 100, Harrisonville, MO 64701.

33. Defendant Cobblestone Family Medicine Clinic d/b/a Clay Platte Family Medicine Clinic P.C. is, upon information and belief, a Missouri Corporation with its headquarters in Liberty, Missouri. Defendant can be served at its Registered Address at 117 S Lexington St., Ste. 100, Harrisonville, MO 64701.

34. Defendant Barry Pointe Family Care, LLC d/b/a Barry Pointe Family Care is, upon information and belief, a Missouri Corporation with its headquarters in Kansas City, Missouri. Defendant can be served at its Registered Address at 9151 NE 81st Terrace, Ste. 100, Kansas City, MO 64158.

BACKGROUND FACTS

35. Certain allegations are made upon information and belief.

36. Defendants are, upon information and belief, healthcare providers and family medicine clinics located throughout Missouri.

37. As a part of its business operations, Defendants collects and maintains PHI and PII of its patients.

38. Plaintiffs and the Class Members are and/or were patients of Defendants and, as a result, provided their PHI and PII to Defendants.

39. Plaintiffs and the Class Members entered into an implied contract with Defendants for the adequate protection of their PHI and PII.

40. Defendants is required to maintain the strictest privacy and confidentiality of Plaintiffs and the proposed Classes' PHI and PII.

41. Defendants fail to post their privacy practices online, in violation of their obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

42. On or about September 21, 2024, Defendants published an online notice (the "Notice") alerting its patients of the data breach stating:

> On June 26, 2024, Clay Platte Family Medicine, along with the providers they share patients with—Summit Family and Sports Medicine Clinic, Cobblestone Family Medicine Clinic, and Barry Pointe Family Medicine Clinic ("the Clinics")—detected suspicious activity in their network environment. Upon discovery of this incident, the Clinics promptly took steps to secure their network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, the Clinics learned that an unauthorized actor potentially accessed and acquired certain files and data stored within their network.
>
> Upon learning this, the Clinics launched a review of the potentially affected data to identify the individuals and information involved. On

> September 10, 2024, the Clinics identified persons whose personal health information ("PHI") was potentially included within the impacted data.

43. Upon information and belief, the cyberattack was targeted at Defendants, due to its status as a healthcare entity that collects, creates, and maintains PHI and PII on its computer networks and/or systems.

44. Although Defendants downplay the incident with qualifiers like "potentially" and "may," they are aware that cybercriminals intentionally targeted Defendants for the highly sensitive Private Information they store on their computer network, attacked, and bypassed the insufficiently secured network, and exfiltrated the highly sensitive Private Information of victims. As a result, the Private Information of Plaintiffs and Class Members remain in the hands of those cyber-criminals.

45. Indeed, Defendants' notification letters to Plaintiffs provided no information regarding the Data Breach except that they discovered the malicious activity on June 26, 2024, and yet failed to even identify the persons affected until September 10, 2024.

46. Given that it took Defendants nearly three months to even figure out who was affected and then another month to simply send letters, it is likely that Defendants failed to implement and properly test a sufficient cybersecurity incident response plan, which is an elementary aspect of any reasonable cybersecurity program. If Defendants cannot even get this basic aspect of a cybersecurity program right, it speaks volumes about the sufficiency of the more technical aspects of its cybersecurity preparedness.

47. Further, Defendants still have not disclosed when the hack actually began or how long the hackers were inside Defendants' information systems. Given that Plaintiffs

cannot assume that Defendants are purposefully hiding information, Plaintiffs reasonably infer that Defendants simply do not know this information, which strongly implies that Defendants lacked the appropriate monitoring, alerting, and intrusion detection systems that are essential to identifying malicious activity before hackers have the opportunity to infiltrate a company's information systems and download their files.

48. The disclosure of the PHI and PII at issue was a result of the Defendants' inadequate safety and security protocols governing PHI and PII and its intent to profit off the use and disclosure of Plaintiffs' and the Class Members' PHI and PII.

49. Upon information and belief, the Breach affected tens of thousands of Defendants' patients.

50. As a direct and/or proximate result of Defendants' failure to properly safeguard and protect the PHI and PII of its patients, Plaintiffs' and the other Class Members' PHI and PII was stolen, compromised and wrongfully disseminated without authorization.

51. Defendants had a duty to their patients to protect them from wrongful disclosures.

52. As a business offering health insurance services, Defendants is required to train and supervise its employees and agents regarding the policies and procedures as well as the State and Federal laws for safeguarding patient information.

53. Defendants are covered entities pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendants must therefore

comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

54. Defendants are covered entities pursuant to the Health Information Technology Act ("HITECH").[1] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

55. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy in Missouri. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

56. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy in Missouri. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

57. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

58. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. *See* 42 C.F.R. §§ 164.302-164.318.

[1] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

59. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

60. HIPAA requires a covered entity or business associate 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. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

61. HIPAA requires a covered entity or business associate 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).

62. Under HIPAA:

> Protected health information means individually identifiable health information:
>
> (1) Except as provided in paragraph (2) of this definition, that is:
>
> (i) Transmitted by electronic media;
>
> (ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.[2]

63. HIPAA and HITECH obligated Defendants to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

64. 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.

65. HIPAA further obligated Defendants to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

66. 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

[2] 45 C.F.R. § 160.103.

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." *See* US Department of Health & Human Services, Security Rule Guidance Material.[3] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represents the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[4]

67. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (*e.g.*, whether the incident involved sensitive information like social security numbers or infectious disease test results);
>
> (2) the recipient of the PHI;
>
> (3) whether the PHI was actually acquired or viewed; and

[3] U.S. Dep't of Health and Human Servs., *Security Rule Guidance Material* (Oct. 24, 2024), http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[4] U.S. Dep't of Health and Human Servs., *Guidance on Risk Analysis* (July 22, 2019), https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

(4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (*e.g.*, whether it was immediately sequestered and destroyed)."[5]

68. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

69. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their rolls in facility security.

70. Defendants failed to provide proper notice to Plaintiffs and the Class Members of the disclosure.

71. Defendants failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

72. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, the criminal(s) and/or their patients now have Plaintiffs' and the other Class Members' compromised PHI and PII.

73. There is a robust international market for the purloined PHI and PII, specifically medical information. Defendants' wrongful actions and/or inaction and the

[5] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304.

resulting Breach have also placed Plaintiffs and the other Classes at an imminent, immediate and continuing increased risk of identity theft, identity fraud[6] and medical fraud.

74. Identity theft occurs when someone uses an individual's PHI and PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* Federal Trade Commission, *Fighting Back against Identity Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited Jan. 18, 2013). The Federal Trade Commission estimates that the identities of as many as nine million Americans are stolen each year. *Id.*

75. The Federal Trade Commission correctly sets forth that "Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit." *Id.*

76. Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (such as obtaining a driver's license or official identification card in the victim's name but with their picture), using a victim's name and Social Security number to obtain government benefits and/or filing a fraudulent tax return using a victim's information. Identity thieves also obtain jobs using stolen Social Security

[6] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

numbers, rent houses and apartments and/or obtain medical services in a victim's name. Identity thieves also have been known to give a victim's PHI and PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

77. According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[7] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[8]

78. According to the Javelin Report, in 2011, the mean consumer cost of rectifying identity fraud was $354 while the mean resolution time of identity fraud was 12 hours. *Id.* at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *Id.* at 9. Consumers who received a data breach notification had a fraud incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *Id.* at 10. More important, consumers who were notified

[7] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012 http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[8] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35-38 (Dec. 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12.

that their PHI and PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *Id.* at 39.

79. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse. *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html). Thus, a person whose PHI and/or PII has been stolen cannot obtain a new Social Security number until the damage has already been done.

80. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems; because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

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

82. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other Private Information, such as your name and address, remains the same."[9]

83. Defendants' data security obligations were also particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

84. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[10]

85. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

86. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods.

---

[9] Social Security Admin., *Identity Theft and Your Social Security Number*, Pub. No. 05-10064 (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[10] Advent Health Univ., *5 Important Elements to Establish Data Security in Healthcare* (May 21, 2020), https://www.ahu.edu/blog/data-security-in-healthcare.

See www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html. For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. "Victims of medical identity theft [also] may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits." *Id.*

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

88. According to the U.S. Department of Health and Human Services, "Ransomware and hacking are the primary cyber-threats in health care." Ransomware cyberattacks reported to the U.S. Dept. of Health and Human Services, Office for Civil Rights have increased 278% from 2018-2023.[12]

89. A study of ransomware cyberattacks from 2016-2023 on healthcare organizations in the U.S. found: 539 individual ransomware attacks on healthcare

[11] Steve Adler, *Editorial: Why Do Criminals Target Medical Records*, THE HIPAA JOURNAL (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[12] U.S. Dep't of Health and Human Servs., *HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation*, (Oct. 31, 2023), https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html.

organizations; 9,780 healthcare organizations affected; Approximately 52.3 million individual patient records impacted; Ransomware demands varying from $1,600 to $10 million; Average downtime across all years of 14 days, with a total of 6,347 days of downtime; Hackers receiving payment in 31 out of 160 cases where the healthcare organization "disclosed whether or not they paid the ransom"; and Overall cost of the attacks of approximately $77.5 billion in downtime alone.[13]

90. In 2023 alone, 46 hospital systems suffered ransomware attacks in 2023, which affected 141 hospitals directly affected, wherein patient care was disrupted "due to the lack of access to IT systems and patient data."[14]

91. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[15]

92. The HIPAA Journal article goes on to explain that patient records, like those stolen from Ascension, are "often processed and packaged with other illegally obtained data to create full record sets (the previously mentioned Fullz package) that contain extensive information on individuals, often in intimate detail." The record sets are then

[13] Paul Bischoff, *Ransomware Attacks on Healthcare Organizations Have Cost the US Economy $77.5bn in Downtime Alone*, Comparitech, (Oct. 23, 2023), https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data.
[14] Steve Adler, *At Least 141 Hospitals Directly Affected by Ransomware Attacks in* 2023, THE HIPAA JOURNAL, (JAN. 4, 2024) https://www.hipaajournal.com/2023-healthcare-ransomware-attacks.
[15] Steve Adler, *Editorial: Why Do Criminals Target Medical Records*, THE HIPAA JOURNAL (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records.

sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[16]

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

94. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[17]

95. These significant increases in attacks to companies, particularly those in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendants.

96. A study by Experian found that the average total cost of medical identity theft is "nearly $13,500" per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.[18] Victims of healthcare data breaches often find themselves "being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores."[19]

---

[16] *Id.*

[17] Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

[18] Brian O'Connor, *Health Care 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.

[19] *Id.*

97. Moreover, 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.

98. It is incorrect to assume that reimbursing a victim for a financial loss due to fraud makes that individual whole again. Like the GAO's study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems."[20] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."[21]

99. As the fraudulent activity resulting from the Data Breach may not come to light for years, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

[20] Erika Harrell, *Victims of Identity Theft, 2014*, U.S. DEP'T OF JUSTICE (Sept. 2015), https://bjs.ojp.gov/content/pub/pdf/vit14.pdf (revised Nov. 13, 2017).
[21] *Id.*

Defendants Failed to Comply with FTC Guidelines.

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

101. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[22]

102. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

103. 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

[22] Federal Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

105. Defendants failed to properly implement basic 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, 15 U.S.C. § 45.

Defendants Failed to Comply with Industry Standards.

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

107. To prevent and detect unauthorized cyber-attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the

end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with at least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[23]

108. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications,

[23] *Id.* at 3–4.

which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[24]

109. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

[24] Cybersecurity and Infrastructure Security Agency, *Protecting Against Ransomware* (April 11, 2019), https://www.cisa.gov/news-events/news/protecting-against-ransomware (revised Sept. 2, 2021).

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[25]

110. Defendants made the choice to collect and store the Private Information of Plaintiffs and Class Members, and therefore could and should have implemented all the above measures to prevent and detect cyberattacks.

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

[25] Microsoft Threat Intelligence, *Human-Operated Ransomware Attacks: A Preventable Disaster*, (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster.

112. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

113. Defendants flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiffs' and the other Class Members' prior written consent to disclose their PHI and PII to any other person—as required by laws, regulations, industry standards and/or internal company standards.

114. Defendants flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons.

115. Upon information and belief, Defendants flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy and property rights, and harmed them in the process, by failing to keep or maintain an accurate accounting of the PHI and PII wrongfully disclosed in the Breach.

116. Defendants flagrantly disregarded and/or violated Plaintiffs' and the other Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and the other Class Members' PHI and PII to protect against anticipated threats to the security or integrity of such information. Defendants' unwillingness or inability to establish and maintain the proper information

security procedures and controls is an abuse of discretion and confirms its intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

117. The actual harm and adverse effects to Plaintiffs and the other Class Members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendants' above wrongful actions and/or inaction and the resulting Breach requires Plaintiffs and the other Class Members to take affirmative acts to recover their peace of mind, and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts—for which there is a financial and temporal cost. Plaintiffs and the other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

118. Victims and potential victims of identity theft, identity fraud and/or medical fraud—such as Plaintiffs and the other Class Members—typically spend hundreds of hours in personal time and hundreds of dollars in personal funds to resolve credit and other financial issues resulting from data breaches. *See Defend: Recover from Identity Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/defend.html; *Fight Identity Theft*, www.fightidentitytheft.com. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for data breach victims, those who are further victimized by identity theft or identity fraud will incur an average

fraud-related economic loss of $1,513 and incur an average of $354 of out-of-pocket expenses attempting to rectify the situation. *Id*. at 6.

119. Other statistical analyses are in accord. The GAO found that identity thieves use PHI and PII to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PHI and PII, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

120. Defendants' wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiffs' and the other Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiffs and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) identity theft, (iii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and/or medical fraud, (iv) out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other Breach risk mitigation products, (v) out-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach, including the costs of placing a credit

freeze and subsequently removing a credit freeze, (vi) the value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach and (vii) the lost benefit of their bargain when they paid for their privacy to be protected and it was not.

PLAINTIFFS' EXPERIENCES

Plaintiff T.R.

121. As stated above, Plaintiff T.R. is a resident and citizen of the State of Florida and the United States of America.

122. In the course of obtaining treatment, Plaintiff T.R. was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Defendants with her PII and PHI, Plaintiff T.R. reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

123. In the course of obtaining treatment, Plaintiff T.R. received a copy of Defendants' Notice of Privacy Practices.

124. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

125. As a result of the Data Breach, Plaintiff T.R. has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis;

reviewing and remaining vigilant against medical fraud. Plaintiff T.R. has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff T.S. has already been notified by her credit monitoring service that her PII and PHI has been disseminated on the Dark Web.

126. To date, Plaintiff T.R. has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff T.R. values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

127. Had Plaintiff T.R. been informed of Defendants' insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff T.R. has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff T.S. anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

128. Plaintiff T.R. suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory

damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of her life; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

131. Plaintiff T.R. has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

132. Upon information and belief, Defendants continue to store and/or share Plaintiff T.R.'s PII and PHI on its internal systems. Thus, Plaintiff T.R. has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff D.S.

133. As stated above, Plaintiff D.S. is a resident and citizen of the State of Missouri and the United States of America.

134. In the course of obtaining treatment, Plaintiff D.S. was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of

birth, and address. When providing and entrusting Defendants with her PII and PHI, Plaintiff T.S. reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

135. In the course of obtaining treatment, Plaintiff D.S. received a copy of Defendants' Notice of Privacy Practices.

136. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

137. As a result of the Data Breach, Plaintiff D.S. has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff D.S. has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff D.S. has already been notified by her credit monitoring service that her PII and PHI has been disseminated on the Dark Web.

138. To date, Plaintiff D.S. has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff D.S. values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

139. Had Plaintiff D.S. been informed of Defendants' insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff D.S. has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff D.S. anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

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

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

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

143. Plaintiff D.S. has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

144. Upon information and belief, Defendants continue to store and/or share Plaintiff D.S.'s PII and PHI on its internal systems. Thus, Plaintiff D.S. has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff T.S.

145. As stated above, Plaintiff T.S. is a resident and citizen of the State of Kansas and the United States of America.

146. In the course of obtaining treatment, Plaintiff T.S. was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Defendants with her PII and PHI, Plaintiff T.S. reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

147. In the course of obtaining treatment, Plaintiff T.S. received a copy of Defendants' Notice of Privacy Practices.

148. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

149. As a result of the Data Breach, Plaintiff T.S. has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited

to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff T.S. has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff T.S. has already been notified by her credit monitoring service that her PII and PHI has been disseminated on the Dark Web.

150. To date, Plaintiff T.S. has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff T.S. values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

151. Had Plaintiff T.S. been informed of Defendants' insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff T.S. has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff T.S. anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

152. Plaintiff T.S. suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and

opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of her life; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

155. Plaintiff T.S. has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

156. Upon information and belief, Defendants continue to store and/or share Plaintiff T.S.'s PII and PHI on its internal systems. Thus, Plaintiff T.S. has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Breanna Highfill

157. As stated above, Plaintiff Highfill is a resident and citizen of the State of Missouri and the United States of America.

158. In the course of obtaining treatment, Plaintiff was required, directly or indirectly, to provide PII and PHI, including Plaintiff's name, Social Security number, date of birth, and address. When providing and entrusting Defendants with PII and PHI, Plaintiff reasonably expected that all PII and PHI would remain safe and not be accessed by unauthorized third parties.

159. In the course of obtaining services from Defendants, Plaintiff received a copy of Defendants' Notice of Privacy Practices.

160. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

161. As a result of the Data Breach, Plaintiff has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring Plaintiff's credit card and other financial statements for any signs of fraudulent activity; monitoring credit reports; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

162. To date, Plaintiff has spent time on efforts to react to and protect against the harm resulting from the Data Breach. Plaintiff values privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

163. Had Plaintiff been informed of the insufficient data security measures protecting the PII and PHI held by Defendants, Plaintiff would not have willingly provided PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

164. Plaintiff has suffered actual injury from having highly sensitive PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of Plaintiff's life; and (x) the continued and certainly increased risk to Plaintiff's PII and PHI, 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 fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

167. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

168. Upon information and belief, Defendants continue to store and/or share Plaintiff's PII and PHI on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

169. Plaintiff's USAA account was compromised around August of 2024. This is the account from which she paid for Defendants' services.

Plaintiff Charles Leap

170. As stated above, Plaintiff Charles Leap is a resident and citizen of the State of Missouri and the United States of America.

171. In the course of obtaining treatment, Plaintiff was required, directly or indirectly, to provide PII and PHI, including Plaintiff's name, Social Security number, date of birth, and address. When providing and entrusting Defendants with PII and PHI, Plaintiff reasonably expected that all PII and PHI would remain safe and not be accessed by unauthorized third parties.

172. In the course of obtaining services from Defendants, Plaintiff received a copy of Defendants' Notice of Privacy Practices.

173. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

174. As a result of the Data Breach, Plaintiff has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring Plaintiff's credit card and other financial statements for any signs of fraudulent activity; monitoring credit reports; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

175. To date, Plaintiff has spent time on efforts to react to and protect against the harm resulting from the Data Breach. Plaintiff values privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

176. Had Plaintiff been informed of the insufficient data security measures protecting the PII and PHI held by Defendants, Plaintiff would not have willingly provided PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data

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

177. Plaintiff has suffered actual injury from having highly sensitive PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of Plaintiff's life; and (x) the continued and certainly increased risk to Plaintiff's PII and PHI, 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 fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

180. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

181. Upon information and belief, Defendants continue to store and/or share Plaintiff's PII and PHI on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Rachel Taylor

182. As stated above, Plaintiff Rachel Taylor is a resident and citizen of the State of Missouri and the United States of America.

183. In the course of obtaining treatment, Plaintiff was required, directly or indirectly, to provide PII and PHI, including Plaintiff's name, Social Security number, date of birth, and address. When providing and entrusting Defendants with PII and PHI, Plaintiff reasonably expected that all PII and PHI would remain safe and not be accessed by unauthorized third parties.

184. In the course of obtaining services from Defendants, Plaintiff received a copy of Defendants' Notice of Privacy Practices.

185. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

186. As a result of the Data Breach, Plaintiff has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring Plaintiff's credit card and other financial statements for any signs of fraudulent activity; monitoring credit reports; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other

activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

187. To date, Plaintiff has spent time on efforts to react to and protect against the harm resulting from the Data Breach. Plaintiff values privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

188. Had Plaintiff been informed of the insufficient data security measures protecting the PII and PHI held by Defendants, Plaintiff would not have willingly provided PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

189. Plaintiff has suffered actual injury from having highly sensitive PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of Plaintiff's life; and (x) the continued and certainly increased risk to Plaintiff's PII and PHI, 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 fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

192. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

193. Upon information and belief, Defendants continue to store and/or share Plaintiff's PII and PHI on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Travis Taylor

194. As stated above, Plaintiff Travis Taylor is a resident and citizen of the State of Missouri and the United States of America.

195. In the course of obtaining treatment, Plaintiff was required, directly or indirectly, to provide PII and PHI, including Plaintiff's name, Social Security number, date of birth, and address. When providing and entrusting Defendants with PII and PHI, Plaintiff reasonably expected that all PII and PHI would remain safe and not be accessed by unauthorized third parties.

196. In the course of obtaining services from Defendants, Plaintiff received a copy of Defendants' Notice of Privacy Practices.

197. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

198. As a result of the Data Breach, Plaintiff has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring Plaintiff's credit card and other financial statements for any signs of fraudulent activity; monitoring credit reports; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

199. To date, Plaintiff has spent time on efforts to react to and protect against the harm resulting from the Data Breach. Plaintiff values privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

200. Had Plaintiff been informed of the insufficient data security measures protecting the PII and PHI held by Defendants, Plaintiff would not have willingly provided PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data

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

201. Plaintiff has suffered actual injury from having highly sensitive PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of Plaintiff's life; and (x) the continued and certainly increased risk to Plaintiff's PII and PHI, 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 fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

204. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

205. Upon information and belief, Defendants continue to store and/or share Plaintiff's PII and PHI on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff K.H.

206. As stated above, Plaintiff K.H. is a resident and citizen of the State of Missouri and the United States of America.

207. In the course of obtaining treatment, Plaintiff was required, directly or indirectly, to provide PII and PHI, including Plaintiff's name, Social Security number, date of birth, and address. When providing and entrusting Defendants with PII and PHI, Plaintiff reasonably expected that all PII and PHI would remain safe and not be accessed by unauthorized third parties.

208. In the course of obtaining services from Defendants, Plaintiff received a copy of Defendants' Notice of Privacy Practices.

209. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

210. As a result of the Data Breach, Plaintiff has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring Plaintiff's credit card and other financial statements for any signs of fraudulent activity; monitoring credit reports; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other

activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

211. To date, Plaintiff has spent time on efforts to react to and protect against the harm resulting from the Data Breach. Plaintiff values privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

212. Had Plaintiff been informed of the insufficient data security measures protecting the PII and PHI held by Defendants, Plaintiff would not have willingly provided PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

213. Plaintiff has suffered actual injury from having highly sensitive PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of Plaintiff's life; and (x) the continued and certainly increased risk to Plaintiff's PII and PHI, 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 fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

216. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

217. Upon information and belief, Defendants continue to store and/or share Plaintiff's PII and PHI on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

218. Furthermore, Plaintiff K.H. incurred fraudulent charges on her bank account on or around January 2, 2025.

Plaintiff H.F.

219. As stated above, Plaintiff H.F. is a resident and citizen of the State of Missouri and the United States of America.

220. In the course of obtaining treatment, Plaintiff was required, directly or indirectly, to provide PII and PHI, including Plaintiff's name, Social Security number, date of birth, and address. When providing and entrusting Defendants with PII and PHI, Plaintiff

reasonably expected that all PII and PHI would remain safe and not be accessed by unauthorized third parties.

221. In the course of obtaining services from Defendants, Plaintiff received a copy of Defendants' Notice of Privacy Practices.

222. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

223. As a result of the Data Breach, Plaintiff has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring Plaintiff's credit card and other financial statements for any signs of fraudulent activity; monitoring credit reports; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

224. To date, Plaintiff has spent time on efforts to react to and protect against the harm resulting from the Data Breach. Plaintiff values privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

225. Had Plaintiff been informed of the insufficient data security measures protecting the PII and PHI held by Defendants, Plaintiff would not have willingly provided PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff has already suffered

injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

226. Plaintiff has suffered actual injury from having highly sensitive PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of Plaintiff's life; and (x) the continued and certainly increased risk to Plaintiff's PII and PHI, 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 fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

229. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

230. Upon information and belief, Defendants continue to store and/or share Plaintiff's PII and PHI on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff David Dempsey

231. As stated above, Plaintiff Dempsey is a resident and citizen of the State of Missouri and the United States of America.

232. In the course of obtaining treatment, Plaintiff was required, directly or indirectly, to provide PII and PHI, including Plaintiff's name, Social Security number, date of birth, and address. When providing and entrusting Defendants with PII and PHI, Plaintiff reasonably expected that all PII and PHI would remain safe and not be accessed by unauthorized third parties.

233. In the course of obtaining services from Defendants, Plaintiff received a copy of Defendants' Notice of Privacy Practices.

234. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

235. As a result of the Data Breach, Plaintiff has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring Plaintiff's credit card and other financial statements for any signs of fraudulent activity; monitoring

credit reports; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

236. To date, Plaintiff has spent time on efforts to react to and protect against the harm resulting from the Data Breach. Plaintiff values privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

237. Had Plaintiff been informed of the insufficient data security measures protecting the PII and PHI held by Defendants, Plaintiff would not have willingly provided PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

238. Plaintiff has suffered actual injury from having highly sensitive PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of Plaintiff's

life; and (x) the continued and certainly increased risk to Plaintiff's PII and PHI, 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 fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

241. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

242. Upon information and belief, Defendants continue to store and/or share Plaintiff's PII and PHI on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff C.C. on behalf of minor child A.C.

243. As stated above, Plaintiff C.C. is pursuing this matter on behalf of minor child A.C. Both are residents and citizen of the State of Missouri and the United States of America.

244. In the course of obtaining treatment, Plaintiff was required, directly or indirectly, to provide PII and PHI, including Plaintiff's name, Social Security number, date

of birth, and address. When providing and entrusting Defendants with PII and PHI, Plaintiff reasonably expected that all PII and PHI would remain safe and not be accessed by unauthorized third parties.

245. In the course of obtaining services from Defendants, Plaintiff received a copy of Defendants' Notice of Privacy Practices.

246. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

247. As a result of the Data Breach, Plaintiff has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring Plaintiff's credit card and other financial statements for any signs of fraudulent activity; monitoring credit reports; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

248. To date, Plaintiff has spent time on efforts to react to and protect against the harm resulting from the Data Breach. Plaintiff values privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

249. Had Plaintiff been informed of the insufficient data security measures protecting the PII and PHI held by Defendants, Plaintiff would not have willingly provided PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and

its likely subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

250. Plaintiff has suffered actual injury from having highly sensitive PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of Plaintiff's life; and (x) the continued and certainly increased risk to Plaintiff's PII and PHI, 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 fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

253. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

254. Upon information and belief, Defendants continue to store and/or share Plaintiff's PII and PHI on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

255. Plaintiff received notice through credit monitoring services that Plaintiff's PII was posted on the dark web.

Plaintiff Joshua Sartin

256. As stated above, Plaintiff Joshua Sartin is a resident and citizen of the State of Missouri and the United States of America.

257. In the course of obtaining treatment, Plaintiff was required, directly or indirectly, to provide PII and PHI, including Plaintiff's name, Social Security number, date of birth, and address. When providing and entrusting Defendants with PII and PHI, Plaintiff reasonably expected that all PII and PHI would remain safe and not be accessed by unauthorized third parties.

258. In the course of obtaining services from Defendants, Plaintiff received a copy of Defendants' Notice of Privacy Practices.

259. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

260. As a result of the Data Breach, Plaintiff has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited

to: researching and verifying the legitimacy of the Data Breach; monitoring Plaintiff's credit card and other financial statements for any signs of fraudulent activity; monitoring credit reports; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

261. To date, Plaintiff has spent time on efforts to react to and protect against the harm resulting from the Data Breach. Plaintiff values privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

262. Had Plaintiff been informed of the insufficient data security measures protecting the PII and PHI held by Defendants, Plaintiff would not have willingly provided PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

263. Plaintiff has suffered actual injury from having highly sensitive PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of Plaintiff's life; and (x) the continued and certainly increased risk to Plaintiff's PII and PHI, 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 fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

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

266. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

267. Upon information and belief, Defendants continue to store and/or share Plaintiff's PII and PHI on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Maria Dunn

268. As stated above, Plaintiff Dunn is a resident and citizen of the State of Missouri and the United States of America.

269. In the course of obtaining treatment, Plaintiff was required, directly or indirectly, to provide PII and PHI, including Plaintiff's name, Social Security number, date of birth, and address. When providing and entrusting Defendants with PII and PHI, Plaintiff reasonably expected that all PII and PHI would remain safe and not be accessed by unauthorized third parties.

270. In the course of obtaining services from Defendants, Plaintiff received a copy of Defendants' Notice of Privacy Practices.

271. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in their system.

272. As a result of the Data Breach, Plaintiff has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring Plaintiff's credit card and other financial statements for any signs of fraudulent activity; monitoring credit reports; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

273. To date, Plaintiff has spent time on efforts to react to and protect against the harm resulting from the Data Breach. Plaintiff values privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

274. Had Plaintiff been informed of the insufficient data security measures protecting the PII and PHI held by Defendants, Plaintiff would not have willingly provided PII and PHI to Defendants. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

275. Plaintiff has suffered actual injury from having highly sensitive PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the cost of credit monitoring for the remainder of Plaintiff's life; and (x) the continued and certainly increased risk to Plaintiff's PII and PHI, 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 fail to undertake appropriate and adequate measures to protect the PII and PHI.

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

277. Moreover, Plaintiff Dunn has been harassed by a barrage of spam and scam messages since the Data Breach.

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

279. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

280. Upon information and belief, Defendants continue to store and/or share Plaintiff's PII and PHI on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

281. Plaintiff has had an appointment at a hair salon fraudulently booked in her name.

CLASS ACTION ALLEGATIONS

282. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed Nationwide Class and State Subclasses, defined as follows:

> **All persons residing in the United States who were patients of Defendants since June 26, 2019 and whose PHI and/or PII was disclosed by Defendants to unauthorized third-parties (the "Nationwide Class").**
>
> **All persons residing in the State of Missouri who were patients of Defendants since June 26, 2019 and whose PHI and/or PII was disclosed by Defendants to unauthorized third-parties (the "Missouri Class").**

283. Excluded from the Classes 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.

284. Plaintiffs reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

285. Numerosity: On information and belief, the putative Classes are comprised of tens of thousands of individuals making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

286. Commonality and Predominance: The rights of Plaintiffs and each other Class Members were violated in a virtually identical manner as a direct and/or proximate result of Defendants' willful, reckless and/or negligent actions and/or inaction and the resulting Breach. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) Whether Defendants willfully, recklessly and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the other Class Members' PHI and/or PII;

b) Whether Defendants was negligent in failing to properly safeguard and protect Plaintiffs' and the other Class Members' PHI and/or PII;

c) Whether Defendants owed a duty to Plaintiffs and the other Class Members to exercise reasonable care in safeguarding and protecting their PHI and/or PII;

d) Whether Defendants breached their duty to exercise reasonable care in failing to safeguard and protect Plaintiffs' and the other Class Members' PHI and/or PII;

e) Whether Defendants was negligent in failing to safeguard and protect Plaintiffs' and the other Class Members' PHI and/or PII;

f) Whether, by publicly disclosing Plaintiffs' and the other Class Members' PHI and/or PII without authorization, Defendants invaded their privacy; and

g) Whether Plaintiffs and the other Class Members sustained damages as a result of Defendants' failure to safeguard and protect their PHI and/or PII.

287. Adequacy: Plaintiffs and their counsel will fairly and adequately represent the interests of the other Class Members. Plaintiffs has no interests antagonistic to, or in conflict with, the other Class Members' interests. Plaintiffs' lawyers are highly experienced in the prosecution of consumer class action and data breach cases.

288. Typicality: Plaintiffs' claims are typical of the other Class Members' claims in that Plaintiffs' claims and the other Class Members' claims all arise from Defendants' failure to properly safeguard and protect their PHI and PII.

289. Superiority and Manageability: A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs' and the other Class Members' claims. Plaintiffs and the other Class Members have been harmed as a result of Defendants' wrongful actions and/or inaction and the resulting Breach. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct.

290. Class certification, therefore, is appropriate pursuant to Civ. P. Rule 23 because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

291. Policies Generally Applicable to the Case: Class certification also is appropriate pursuant to Civ. P. Rule 23 because Defendants has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

292. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights. Absent a class action, Defendants will retain the benefits of its wrongdoing despite its serious violations of the law.

293. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

294. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

295. Unless a Class-wide injunction is issued, Defendants may continue in its failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data

Breach, and Defendants may continue to act unlawfully as set forth in this First Amended Complaint.

COUNT I
BREACH OF IMPLIED CONTRACT

296. The preceding factual statements and allegations are incorporated herein by reference.

297. Plaintiffs and the other Class Members, as part of their agreement with Defendants, provided Defendants their PHI and PII.

298. In providing such PHI and PII, Plaintiffs and the other Class Members entered into an implied contract with Defendants, whereby Defendants became obligated to reasonably safeguard Plaintiffs' and the other Class members' PHI and PII.

299. Under the implied contract, Defendants was obligated to not only safeguard the PHI and PII, but also to provide Plaintiffs and Class Members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

300. Defendants breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their PHI and PII.

301. Defendants separately breached the implied contract with Plaintiffs and the other Class Members by failing to provide Plaintiffs and Class Members with prompt and adequate notice of the unauthorized access to their PHI and PII.

302. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the other Class Members' confidential medical information, Plaintiffs and the members of the Class suffered damages, including, without

limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

303. Plaintiffs and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and Class members are entitled to nominal damages.

COUNT II
NEGLIGENCE

304. The preceding factual statements and allegations are incorporated herein by reference.

305. Plaintiffs bring this Count on their own behalf and on behalf of the Class.

306. Defendants owed, and continues to owe, a duty to Plaintiffs and the Classes to safeguard and protect their PHI and PII.

307. Defendants breached their duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiffs' and the other Class Members' PHI and PII.

308. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class Members' PHI and PII

would result in an unauthorized third-party gaining access to such information for no lawful purpose.

309. Plaintiffs and the Classes entrusted their PII and PHI to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

310. Defendants has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and the Classes could and would suffer if the PII and PHI were wrongfully disclosed.

311. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiffs and the Classes involved an unreasonable risk of harm to Plaintiffs and the Classes, even if the harm occurred through the criminal acts of a third party.

312. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII and PHI of Plaintiffs and the Classes in Defendants' possession was adequately secured and protected.

313. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former patients', employees', and physicians' PII and PHI that Defendants was no longer required to retain pursuant to regulations.

314. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiffs and the Classes.

315. Defendants' duty to use reasonable security measures arose as a result of the contractual relationship that existed between Defendants and Plaintiffs and the Classes.

316. Defendants was also subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Classes.

317. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Classes was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

318. Plaintiffs and the Classes were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiffs and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting PII and PHI stored on Defendants' systems.

319. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the Classes.

320. Defendants' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiffs and the Classes, including basic encryption techniques freely available to Defendants.

321. Plaintiffs and the Classes had no ability to protect their PII and PHI that was in, and possibly remains in, Defendants' possession.

322. Defendants was in a position to protect against the harm suffered by Plaintiffs and the Classes as a result of the Data Breach. Defendants had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiffs and the Classes within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third-parties.

323. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiffs and the Classes.

324. Defendants has admitted that the PII and PHI of Plaintiffs and the Classes was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

325. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Classes by failing to implement industry standard protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiffs and the Classes during the time the PII and PHI was within Defendants' possession or control.

326. Defendants improperly and inadequately safeguarded the PII and PHI of Plaintiffs and the Classes in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

327. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiffs and the Classes in the face of increased risk of theft.

328. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Classes by failing to have appropriate procedures in place to detect and prevent dissemination of their current and former patients', employees', and physicians' PII and PHI.

329. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Classes the existence and scope of the Data Breach.

330. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the member of the Classes confidential medical information, Plaintiffs and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

331. Plaintiffs and the other Classes suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi)

the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Classes are entitled to nominal damages.

332. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

333. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Classes.

334. Defendants' violation of Section 5 of the FTC Act and Title II of HIPAA, including HIPAA regulations HHS has implemented pursuant to Title II, as well as the standards of conduct established by these statutes and regulations, constitutes negligence per se.

335. Plaintiffs and the Classes are within the class of persons that the FTC Act was intended to protect.

336. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against. The FTC has pursued enforcement

actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Classes.

337. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Classes have suffered and will suffer injury, including but not limited to:

a) actual identity theft;

b) the loss of the opportunity of how their PII and PHI is used;

c) the compromise, publication, and/or theft of their PII and PHI;

d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI;

e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

f) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiffs and the Classes; and

g) costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Classes.

133. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Classes 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.

134. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Classes have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

135. Plaintiffs and the Classes are therefore entitled to damages, including actual and compensatory damages, restitution, declaratory and injunctive relief, and attorney's fees, costs, and expenses.

COUNT III
INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

136. The preceding factual statements and allegations are incorporated herein by reference.

137. Plaintiffs' and the other Classes' PHI and PII was (and continues to be) sensitive and personal private information.

138. By virtue of Defendants' failure to safeguard and protect Plaintiffs' and the other Classes' PHI and PII and the resulting Breach, Defendants wrongfully disseminated Plaintiffs' and the other Class Members' PHI and PII to unauthorized persons.

139. The mental state is met here because—given that data breaches represent a ubiquitous threat to any healthcare company—Defendants if they were paying attention at all must have been substantially certain that their failure to implement reasonable cybersecurity measures would lead to a data breach and the inherent harms to victims that ultimately did result.

140. Moreover, the publicity requirement is met because a well-known exception is in cases in which the disclosure was made to those in a special relationship with Plaintiffs. That is the case here. Defendants' disclosure was made to cybercriminals and identity thieves—exactly the individuals from whom reasonable cybersecurity measures were supposed to protect Plaintiffs.

141. Dissemination of Plaintiffs' and the other Classes' PHI and PII is not of a legitimate public concern; publicity of their PHI and PII was, is and will continue to be offensive to Plaintiffs, the other Class Members and all reasonable people. The unlawful disclosure of same violates public mores.

142. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the members of the Classes confidential medical information, Plaintiffs and the members of the Classes suffered damages,

including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation, and loss of enjoyment of life.

143. Plaintiffs and the other Classes' members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Classes' Members are entitled to nominal damages.

144. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiffs' and the other Classes' Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT IV
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY

145. The preceding factual statements and allegations are incorporated herein by reference.

146. At all times relevant hereto, Defendants owed, and owes, a fiduciary duty to Plaintiffs and the proposed class pursuant to Missouri common law, to keep Plaintiffs' medical and other PHI and PII information confidential.

147. The fiduciary duty of privacy imposed by Missouri law is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530, which requires a covered entity or business associate to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient medical records.

148. Defendants breached their fiduciary duty to Plaintiffs by disclosing Plaintiffs and the other Classes' Members PHI and PII to unauthorized third-parties.

149. As a direct result of Defendants' breach of fiduciary duty of confidentiality and the disclosure of Plaintiffs' confidential medical information, Plaintiffs and the proposed Classes' Members suffered damages.

150. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the member of the Classes confidential medical information, Plaintiffs and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

151. Plaintiffs and the other Classes' Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft

and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Classes' Members are entitled to nominal damages

COUNT V
NEGLIGENT TRAINING AND SUPERVISION

152. The preceding factual statements and allegations are incorporated herein by reference.

153. At all times relevant hereto, Defendants owed and owes a duty to Plaintiffs and the Classes to hire competent employees and agents, and to train and supervise them to ensure they recognize the duties owed to their patients and their parents.

154. Defendants breached their duty to Plaintiffs and the members of the Classes by allowing its employees and agents to give access to patient medical records to an unauthorized user.

155. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the member of the Classes confidential medical information, Plaintiffs and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

156. Plaintiffs and the other Classes members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket

expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Classes' Members are entitled to nominal damages.

157. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiffs' and the other Classes' Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT VI
NEGLIGENCE *PER SE*

158. Plaintiffs incorporates by reference and re-alleges all paragraphs previously alleged herein

159. Plaintiffs were under the medical care of the Defendants.

160. Defendants are covered entities for purposes of HIPAA and HITECH.

161. Plaintiffs are members of the class HIPAA and HITECH were created to protect.

162. Plaintiffs' private health information is the type of information HIPAA and HITECH were created to protect. HIPAA and HITECH were created to protect against the wrongful and unauthorized disclosure of an individual's health information.

163. Defendants gave protected medical information to an unauthorized third-party or unauthorized third-parties without the written consent or authorization of Plaintiffs.

164. Defendants gave protected medical information to unauthorized third-parties without Plaintiffs' oral consent or written authorization.

165. The information disclosed to an unauthorized third-party or unauthorized third-parties included private health information about medical treatment.

166. Alternatively, Defendants violated HIPAA and HITECH in that it did not reasonably safeguard the private health information of Plaintiffs from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements pursuant to HIPAA and HITECH including, but not limited to, 42 C.F.R. §§ 164.302-164.318, 45 C.F.R. § 164.500, *et seq.*, and 42 U.S.C. §17902, and was therefore negligent *per se*.

167. As a direct result of Defendants' negligence, Plaintiffs and the Classes suffered damages and injuries, including, without limitation, loss of the benefit of their bargain, a reduction in value of their private health information, loss of privacy, loss of medical expenses, loss of trust, loss of confidentiality, embarrassment, humiliation, emotional distress, and loss of enjoyment of life.

168. Plaintiffs and the other Classes suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud

pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiffs and the other Classes are entitled to nominal damages.

169. As a direct result of Defendants' negligence, Plaintiffs and the Classes have a significantly increased risk of being future victims of identity theft relative to what would be the case in the absence of the Defendants' wrongful acts.

170. As a direct result of Defendants' negligence, future monitoring, in the form of identity-theft or related identity protection is necessary in order to properly warn Plaintiffs and the Classes of, and/or protect Plaintiffs and the Classes from, being a victim of identity theft or other identity-related crimes. Plaintiffs, individually and on behalf of the Classes, seek actual damages for all monies paid to Defendants in violation of the HIPAA and HITECH. In addition, Plaintiffs seek attorneys' fees.

COUNT VII
INVASION OF PRIVACY

171. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein. Plaintiffs bring this Count on behalf of themselves and on behalf of the Missouri Class (the "Class" for the purposes of this Count).

172. Plaintiffs and the Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

173. Defendants owed a duty to its current and former patients including Plaintiffs and the Classes, to keep their Private Information contained as a part thereof, confidential.

174. Defendants failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiffs and the Classes.

175. Defendants allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiffs and the Classes, by way of Defendants' failure to protect the PII and PHI.

176. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and the Classes is highly offensive to a reasonable person.

177. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class disclosed their Private Information to Defendants as part of their medical care or employment with Defendants, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

179. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

180. 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.

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

182. 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 in that the PII and PHI maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class 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.

COUNT VIII
VIOLATIONS OF MISSOURI MERCHANDISING PRACTICES ACT, MO. REV. STAT. § 407.010, *et seq.*

181. The preceding factual statements and allegations are incorporated herein by reference.

182. RSMo. 407.020 prohibits the use of any "deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or

omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce. . . ."

183. An "unfair practice" is defined by Missouri law, 15 CSR 60-8.020, as any practice which:

> (A) Either-
>
> > 1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or
> >
> > 2. Is unethical, oppressive or unscrupulous; and
>
> (B) Presents a risk of, or causes, substantial injury to consumers.

184. 15CSR 60-8.040 provides that it is "[a]n unfair practice for any person in connection with the advertisement or sale of merchandise to violate the duty of good faith in solicitation, negotiation and performance, or in any manner fail to act in good faith."

185. Plaintiffs and Defendants are "persons" within the meaning of section 407.010 (5).

186. Merchandise is defined by the MMPA, to include the providing of "services" and, therefore, encompasses healthcare services.

187. Efforts to maintain the privacy and confidentiality of medical records are part of the healthcare services associated with a good.

188. Maintenance of medical records are "merchandise" within the meaning of section 407.010(4).

189. Plaintiffs' and the Class' goods and services purchased from Defendants were for "personal, family or household purposes" within the meaning of the Missouri Merchandising Practices Missouri Revised Statutes.

190. As set forth herein, Defendants' acts, practices and conduct violate section 407.010(1) in that, among other things, Defendants have used and/or continues to use unfair practices, concealment, suppression and/or omission of material facts in connection with the advertising, marketing, and offering for sale of services associated with healthcare services. Such acts offends the public policy established by Missouri statute and constitute an "unfair practice" as that term is used in Missouri Revised Statute 407.020(1).

191. Defendants' unfair, unlawful and deceptive acts, practices and conduct include: (1) representing to its patients that it will not disclose their sensitive personal health information to an unauthorized third party or parties; (2) failing to implement security measures such as securing the records in a safe place; and (3) failing to train personnel.

192. Defendants' conduct also violates the enabling regulations for the MMPA because it: (1) offends public policy; (2) is unethical, oppressive and unscrupulous; (3) causes substantial injury to consumers; (4) it is not in good faith; (5) is unconscionable; and (6) is unlawful. *See* Mo Code Regs. Ann tit. 15, Section 60-8.

193. As a direct and proximate cause of Defendants' unfair and deceptive acts, Plaintiffs and members of the Class have suffered damages in that they (1) paid more for medical record privacy protections than they otherwise would have, and (2) paid for medical record privacy protections that they did not receive. In this respect, Plaintiffs and

members of the Class have not received the benefit of the bargain and have suffered an ascertainable loss.

194. Plaintiffs, on behalf of themselves and the Class, seek actual damages for all monies paid to The Clinics in violation of the MMPA. In addition, Plaintiffs seeks attorneys' fees.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Classes proposed in this First Amended Complaint, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

A. Declaring that this action is a proper class action, certifying the Classes as requested herein, designating Plaintiffs as Class Representative and appointing Plaintiffs' counsel as Lead Counsel for the Classes;

B. Declaring that Defendants' conduct was extreme and outrageous;

C. Declaring that Defendants breached their implied contract with Plaintiffs and Classes;

D. Declaring that Defendants negligently disclosed Plaintiffs' and the Classes' Members' PHI and PII;

E. Declaring that Defendants have invaded Plaintiffs' and Classes' Members' privacy;

F. Declaring that Defendants breached their fiduciary duty to Plaintiffs and the Classes;

G. Declaring that Defendants breached their implied contract with Plaintiffs and the Classes;

H. Declaring that Defendants were negligent by negligently training and supervising its employees and agents;

I. Declaring that Defendants were negligent by negligently training and

supervising its employees and agents;

J. Ordering Defendants to pay actual damages to Plaintiffs and the Classes;

K. Ordering Defendants to properly disseminate individualized notice of the Breach to all Classes;

L. For an Order enjoining Defendants from continuing to engage in the unlawful business practices alleged herein;

M. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiffs and the Classes;

N. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

O. Ordering such other and further relief as may be just and proper.

Respectfully submitted,

/s/Maureen M. Brady

Maureen M. Brady MO #57800
Lucy McShane MO #57957
MCSHANE & BRADY, LLC
4006 Central Kansas City, MO 64111
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com

Counsel for Plaintiffs TR, DS, and TS

Domenica M. Russo – Mo. Bar # 74819
Brandon M. Wise – Mo. Bar #67242
PEIFFER WOLF CARR
KANE CONWAY & WISE. LLP
One U.S. Bank Plaza, Suite 1950
St. Louis, MO 63101
Telephone: 314-833-4827
Email: drusso@peifferwolf.com

Email: bwise@peifferwolf.com

Eduard Korsinsky*
Mark Svensson*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: ek@zlk.com
Email: msvensson@zlk.com

**pro hac vice* forthcoming

Counsel for Plaintiff Highfill

Nicholas A. Migliaccio*
nmigliaccio@classlawdc.com
Jason S. Rathod*
jrathod@classlawdc.com
MIGLIACCIO & RATHOD LLP
412 H Street NE, no. 302,
Washington, DC, 20002
Office: (202) 470-3520

* *pro hac vice* forthcoming

Counsel for Plaintiff Leap

Domenica M. Russo – Mo. Bar # 74819
Brandon M. Wise – Mo. Bar #67242
PEIFFER WOLF CARR
KANE CONWAY & WISE. LLP
One U.S. Bank Plaza, Suite 1950
St. Louis, MO 63101
Telephone: 314-833-4827
Email: drusso@peifferwolf.com
Email: bwise@peifferwolf.com

Daniel O. Herrera*
Nickolas J. Hagman*
Alex Lee*
CAFFERTY CLOBES MERIWETHER

& SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
alee@caffertyclobes.com

* *Pro Hac Vice* forthcoming

Attorneys for Plaintiffs Rachel and Travis Taylor

NORMAN & GRAVES LLC

Phyllis A. Norman, MO #55887
4505 Madison Avenue, Suite 220
Kansas City, MO 64111
(816) 895-8989
(816) 895-8988 FAX
phyllis@ngkclaw.com

BURGESS LAW FIRM, P.C.
Mitchell L. Burgess, MO #47524
4505 Madison Avenue, Suite 200
Kansas City, MO 64111
(816) 471-1700
(816) 471-1701 FAX
mitch@burgesslawkc.com

Attorneys for Plaintiffs K.H. and H.F.

John F. Garvey, #35879
Colleen Garvey, #72809
Ellen A. Thomas, #73049
STRANCH, JENNINGS & GARVEY, PLLC
Peabody Plaza
701 Market Street, Suite 1510
St. Louis, MO 63101
Tel: (314) 390-6750
jgarvey@stranchlaw.com
cgarvey@stranchlaw.com

ethomas@stranchlaw.com

J. Gerard Stranch, IV*
Grayson Wells (MO 73068)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

**To Seek Pro Hac Vice Admission*

Attorneys for Plaintiffs Dempsey and Dunn

Norman E. Siegel MO# 44378
J. Austin Moore MO# 64040
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com

Jeff Ostrow (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW P.A.
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
E: ostrow@kolawyers.com

Attorneys For Plaintiff C.C. and A.C.

Tiffany Marko Yiatras, #58197
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Tele: 314-541-0317
Email: *tiffany@consumerprotectionlegal.com*

Philip J. Krzeski*

CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
pkrzeski@chestnutcambronne.com

* Motions for Pro Hac Admission to be filed

Attorneys for Plaintiff Sartin