UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

M.S. and D.H., individually and on behalf of all others similarly situated,

Plaintiffs,

v.

MED-DATA, Inc.,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

Plaintiffs M.S. and D.H. ("Plaintiffs"), individually and on behalf of all other similarly situated individuals, and by and through their undersigned counsel files this Class Action Complaint against Defendant Med-Data Inc. ("Med-Data" or "Defendant") and allege the following based upon their personal knowledge of the facts, and upon information and belief based on the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. With this action, Plaintiffs and the "Class" (defined below) seek to hold Defendant responsible for the harms it caused them resulting from the massive and preventable disclosure of medical information that took place sometime between December 2018 and September 2019 through December 17, 2020, during which highly sensitive Med-Data files had been uploaded and saved to a public-facing website (the "Healthcare Data Breach" or the "Breach").[1]

2. As a result of Defendant's negligent and wrongful conduct, Plaintiffs' and Class members' highly confidential and sensitive personal and health information was left exposed to the public eye, in an unencrypted and unprotected format, for more than a year's time.

3. Med-Data, founded in 1980, is a full-service healthcare revenue cycle management services provider that services thousands of hospitals, physicians, and healthcare systems and facilities nationwide.[2]

4. The services offered by Med-Data include processing Medicaid eligibility, third-party liability, workers' compensation, and patient billing for its clients.

[1]The Healthcare Data Breach appears on the U.S. Department of Health and Human Services' online public breach tool showing that 135,908 were potentially impacted by the Healthcare Data Breach. *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed April 29, 2021).

[2] https://www.meddata.com/about-us/patient-financial-life-cycle-services/ (last accessed April 29, 2021).

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

5. In order to provide these services, Med-Data takes possession of its clients' patients' Protected Health Information ("PHI") and Personal Identifiable Information ("PII") (defined below), with the assurance that such information will be kept safe from unauthorized access. By taking possession and control of Plaintiffs' and Class members' PHI and PII, Defendant assumes a duty to securely store and protect the PHI and PII of Plaintiffs and the Class.

6. Defendant breached this duty and betrayed the trust of its clients, Plaintiffs and Class members by failing to properly safeguard and protect their PHI and PII, thus enabling cyber criminals to steal and misuse it.

7. The PHI and PII that was exposed in the Healthcare Data Breach includes: (i) patient contact information (such as patient names, addresses, and dates of birth); (2) Social Security numbers; (3) diagnoses; (4) medical conditions; (5) claims information; (6) dates of service; (7) subscriber IDs; (8) medical procedure codes; (9) provider names; and (10) health insurance policy numbers.[3]

8. Defendant's misconduct – failing to implement adequate and reasonable data security measures to protect Plaintiffs' and Class members' PHI and PII, failing to timely detect the Healthcare Data Breach, failing to take adequate steps to prevent and stop the Healthcare Data Breach, failing to disclose the material facts that it did not have adequate security practices and employee training in place to safeguard the PHI and PII, failing to honor its promises and representations to protect Plaintiffs' and Class members' PHI and PII, and failing to provide timely and adequate notice of the Healthcare Data Breach – caused substantial harm and injuries to Plaintiffs and Class members across the United States.

[3] https://www.hipaajournal.com/vendor-data-breach-involved-publication-of-phi-from-multiple-covered-entities-on-github/#:~:text=Med%2DData%20Inc.%20has%20confirmed,been%20accessed%20by%20unauthorized%20individuals (last accessed April 29, 2021).

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

9. Due to Defendant's negligence and data security failures, cyber criminals had access to and now potentially possess everything they need to commit personal and medical identity theft and wreak havoc on the financial and personal lives of 135,000 individuals.

10. As a result of the Healthcare Data Breach, Plaintiffs and Class members have already suffered damages. For example, now that their PHI and PII has been released into the criminal cyber domains, Plaintiffs and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiffs and Class members are now forced to deal with the danger of identity thieves possessing and fraudulently using their PHI and PII. Plaintiffs have already been the victims of such fraudulent use of their PHI and PII, as detailed below. Additionally, Plaintiffs and Class members have lost time and money responding to and attempting to mitigate the impact of the Healthcare Data Breach.

11. Plaintiffs bring this action individually and on behalf of the Class and seek actual damages, statutory damages, punitive damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices), reasonable attorney's fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

THE PARTIES

Plaintiff M.S.

12. Plaintiff M.S. is a citizen and resident of Shawnee, Kansas.

13. Plaintiff M.S. is a patient of, and received medical services from, AdventHealth Shawnee Mission, one of Defendant's clients.

14. M.S. received a letter from Med-Data dated March 31, 2021 advising that M.S.'s PHI and PII was compromised in the Healthcare Data Breach, including M.S.'s name, Social Security number, physical address, date of birth, telephone number, and medical condition and diagnosis.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

15. As required in order to obtain medical services, M.S. provided highly sensitive personal, health, and insurance information, including the PHI and PII that was compromised in the Healthcare Data Breach. As stated in the letter from Med-Data, Plaintiff M.S.'s PHI and PII was compromised because Med-Data assisted AdventHealth Shawnee Mission with processing M.S.'s claim.

16. Because of Defendant's negligence and failure to train and supervise its employees, which negligence and failure led to the Healthcare Data Breach, M.S.'s PHI and PII have been publicly disclosed. Upon information and belief, the PHI and PII and has already been fraudulently used to harm her.

17. Recently, an unknown third party attempted to impersonate M.S.'s medical transportation. Plaintiff M.S. was suspicious based on the car, which did not appear to be from the medical transportation company, and on the manner of the driver, who was unable to verify that he was affiliated with the company. M.S. called the medical transportation company, who informed M.S. that the driver attempting to transport M.S. was not their employee nor otherwise affiliated with the transportation company. M.S. immediately filed two police reports. Nothing like this had ever happened to Plaintiff M.S. until after the Healthcare Data Breach.

18. Following the Healthcare Data Breach, M.S. has also incurred out of pocket expenses of $161.96 related to the removal of spyware that was recently discovered on M.S.'s laptop.

19. M.S. continues to be under an imminent risk of subsequent identity theft and fraud, including medical identity theft and medical fraud.

20. The imminent risk of medical identity theft and fraud M.S. now faces is substantial, certainly impending, and continuous and ongoing because of the negligence of Defendant in its failure to implement adequate data security protocols and train its employees, which negligence led to the Healthcare Data Breach. Plaintiff M.S. has already spent time and money responding to the Healthcare Data Breach in an attempt to mitigate the harms M.S. has

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

already experienced and will certainly continue to experience in the future as a result of the Breach.

21. As a direct and proximate result of the Healthcare Data Breach, M.S. will need to have identity theft protection for the rest of M.S.'s lifetime.

22. Plaintiff M.S. has suffered additional injury directly and proximately caused by the Healthcare Data Breach, including damages and diminution in the value of M.S.'s PHI and PII that was entrusted to Defendant for the sole purpose of obtaining medical services necessary for M.S.'s health and well-being, with the understanding that Defendant would safeguard this information against unauthorized disclosure. Additionally, M.S.'s PHI and PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendant and is subject to future wrongful disclosures and/or security breaches so long as Defendant fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Plaintiff D.H.

23. Plaintiff D.H. is an adult residing in Kansas City, Missouri, in the County of Jackson County.

24. Plaintiff D.H. was a patient of certain business associates of Defendant and, as a result, provided PHI and PII to Defendant.

25. On March 31, 2021, Defendant sent a letter to Plaintiff D.H. and members of the Class to inform them of a "data security incident" that impacted their PHI and PII.

26. Plaintiff D.H. is now under an imminent risk of subsequent identity theft and fraud, including medical identity theft and medical fraud.

27. The imminent risk of medical identity theft and fraud Plaintiff D.H. now faces is substantial, certainly impending, and continuous and ongoing because of the negligence of Defendant in its failure to implement adequate data security protocols and train its employees, which negligence led to the Healthcare Data Breach. Plaintiff D.H. has already been a victim of

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

fraudulent activity and has spent time and money responding to the Healthcare Data Breach in an attempt to mitigate the harms she has already experienced and will certainly continue to experience in the future as a result of the Breach.

28. As a direct and proximate result of the Healthcare Data Breach, Plaintiff D.H. will need to have identity theft protection for the rest of her lifetime.

29. Plaintiff D.H. has suffered additional injury directly and proximately caused by the Healthcare Data Breach, including damages and diminution in the value of her PHI and PII that was entrusted to Defendant for the sole purpose of obtaining medical services necessary for D.H.'s health and well-being, with the understanding that Defendant would safeguard this information against unauthorized disclosure. Additionally, Plaintiff D.H.'s PHI and PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendant and is subject to future breaches so long as Defendant fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Defendant Med-Data

30. Med-Data, which is incorporated in the State of Washington and has an office in Seattle, Washington, is a full-service healthcare revenue cycle management services provider that services thousands of hospitals, physicians, and healthcare systems and facilities nationwide.

31. The services offered by Med-Data to its clients include, but are not limited to, processing Medicaid eligibility, third-party liability, workers' compensation, and patient billing.

JURISDICTION AND VENUE

32. 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 Plaintiffs and members of the Class are citizens of states that differ from Defendant.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

33. This Court has personal jurisdiction over Defendant because Defendant is incorporated in Washington.

34. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391 because Defendant is incorporated in Washington and is a resident of this District. Defendant conducts business through this District and maintains an office in this District.

FACTUAL ALLEGATIONS

A. The Healthcare Data Breach and Defendant's Failed Response

35. Defendant is at a minimum a business associate of various health care providers and is in receipt of highly sensitive PHI and PII. As such, Defendant is required pursuant to Federal and State law to maintain the strictest confidentiality of its patients and the PHI and PII it receives and collects, and Defendant is further required to maintain sufficient safeguards to protect such PHI and PII from being accessed by unauthorized third parties.

36. Defendant posts its privacy practices online, at https://www.meddata.com/privacy-policy/.

37. On or about December 10, 2020, Defendant was notified by security researcher Jelle Ursem that some of its data had been discovered on the open-source software development hosting website "GitHub" (the "Website").

38. The PHI and PII discovered on the Website was not encrypted.

39. Defendant launched an investigation, which determined that at least one of its employees had saved files containing patients' PHI and PII to the public-facing Website between December 2018 and September 2019. The files were later removed from the Website on December 17, 2020, meaning Plaintiffs' and Class members' PHI and PII was exposed to the world at large for at least thirteen (13) months and potentially longer.

40. Defendant notified its impacted client entities on February 8, 2020, then inexplicably waited an additional seven weeks to notify Plaintiffs and the Class.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

41. Apparently, Defendant needed two months following the completion of its investigation to notify the impacted individuals and provide them with the information and credit monitoring they needed to protect themselves against fraud and identity theft. Defendant was, of course, too late in the discovery and notification of the Healthcare Data Breach.

42. In addition to the severity of the Healthcare Data Breach and the unreasonable amount of time it took for Defendant to finally become aware of it and notify the victims, Defendant has done very little to protect Plaintiffs and the Class. In the Notice letter sent by Med-Data, Defendant encourages them "to remain vigilant against incidents of identity theft…" The Notice also offers Class members a woefully inadequate twelve months of free credit monitoring and identity protection services.

43. In effect, Defendant is shirking its responsibility for the harm and increased risk of harm it has caused Plaintiffs and members of the Class, including the distress and financial burdens the Healthcare Data Breach has placed upon their shoulders.

44. Defendant failed to adequately safeguard Plaintiffs' and Class members' PHI and PII, allowing unauthorized individuals to gain access to this wealth of priceless information for over a year before warning the victims to be on the lookout.

45. Defendant failed to spend sufficient resources on monitoring and training its employees on proper data security protocols.

46. Defendant had obligations created by the Health Insurance Portability and Accountability Act ("HIPAA"), reasonable industry standards, common law, state statutory law, and its assurances and representations to its clients and its clients' patients to keep patients' PHI and PII confidential and to protect such PHI and PII from unauthorized access.

47. Plaintiffs and Class members were required to provide their PHI and PII with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

48. The compromised PHI and PII at issue has great value to criminals due to the large number of individuals affected and the fact that health insurance information, medical information, and Social Security numbers were part of the data that was compromised.

B. Defendant had an Obligation to Protect PHI and PII under Federal Law and the Applicable Standard of Care

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

50. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[4] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

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

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

55. HIPAA's Security Rule requires Defendant to do the following:

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

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

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

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

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

d. Ensure compliance by its workforce.

56. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

57. HIPAA and HITECH also obligated Defendant 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.

58. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Healthcare Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[5]

[5] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

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

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

61. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[6] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[7]

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

[6] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

[7] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

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

64. Defendant owed a duty to Plaintiffs and the Class to create and implement reasonable data security practices and procedures to protect the PHI and PII in its possession, including adequately training its employees and others who accessed Personal Information within its computer systems on how to adequately protect PHI and PII.

65. Defendant owed a duty to Plaintiffs and the Class to implement processes that would detect a compromise of PHI and PII in a timely manner.

66. Defendant owed a duty to Plaintiffs and the Class to act upon data security warnings and alerts in a timely fashion.

67. Defendant owed a duty to Plaintiffs and the Class to disclose whether its computer systems and data security practices were inadequate to safeguard individuals' PHI and PII from theft because such an inadequacy would be a material fact in the decision to entrust PHI and PII with Defendant.

68. Defendant owed a duty to Plaintiffs and the Class to disclose in a timely and accurate manner when data breaches occurred.

69. Defendant owed a duty of care to Plaintiffs and the Class because they were foreseeable and probable victims of any inadequate data security practices.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

C. Defendant was on Notice of Data Threats in the Healthcare Industry and of the Inadequacy of its Data Security

70. Defendant was on notice that companies in the healthcare industry are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information.

71. Defendant was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[8]

72. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[9]

73. As implied by the above AMA quote, stolen PHI and PII can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class members.

---

[8] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[9] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomeware-attacks-shut-down-clinics-hospitals.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

74. Defendant was on notice that the federal government has been concerned about healthcare company data encryption. Defendant knew its employees kept protected health information in their personal files, yet it appears that information was not encrypted.

75. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[10]

76. As a covered entity under HIPAA, Defendant should have known about its data security vulnerabilities and sought better protection for the PHI and PII accumulating in its employees' unprotected files.

D. Cyber Criminals Have and Will Continue to Use Plaintiffs' and Class Members' PHI and PII to Defraud Them

77. Plaintiffs' and Class members' PHI and PII is of great value to cyber criminals, and the data stolen in the Healthcare Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class members and to profit off their misfortune.

78. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[11] For example, with the PHI and PII stolen in the Healthcare Data Breach,

---

[10] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

[11] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[12] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class members.

79. PHI and PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[13]

80. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits in the state of Oklahoma.[14]

81. The PHI and PII exposed in this Healthcare Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[15]

---

[12] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[14] *See* https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; *see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

[15] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

82. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[16]

83. For instance, with a stolen Social Security number, which is only one category of the PHI and PII compromised in the Healthcare Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[17] Identity thieves can also use the information stolen from Plaintiffs and Class members to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

84. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[18]

85. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently

---

[16] *Data Breaches Are Frequent*, *supra* note 11.

[17] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[18] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

discover erroneous information has been added to their personal medical files due to the thief's activities."[19]

86. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where [protected health information] can go from $20 say up to—we've seen $60 or $70 [(referring to prices on dark web marketplaces)]."[20] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[21]

87. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[22] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[23] In other words, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[24]

---

[19] *Id.*

[20] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowedge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[21] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[22] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[23] *Id.*; *see also Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

88. Defendant's failure to offer more than twelve months of free identity theft monitoring to the Class is egregious. One year of identity theft monitoring is woefully inadequate, as the worst is yet to come.

89. With this Healthcare Data Breach, it seems that identity thieves have already started to prey on the victims, and we can anticipate that this will continue.

90. 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.[25] 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."[26]

91. Victims of the Healthcare Data Breach, like Plaintiffs and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Healthcare Data Breach.[27]

92. In fact, as a direct and proximate result of the Healthcare Data Breach, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Healthcare Data Breach

---

[24] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[25] *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html.

[26] *Id.*

[27] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

93. Plaintiffs and the Class have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PHI and PII;

b. Improper disclosure of their PHI and PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PHI and PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Healthcare Data Breach;

f. Loss of privacy suffered as a result of the Healthcare Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PHI and PII; and

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

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

95. Plaintiffs and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the kind of PHI and PII Defendant made so easily accessible to cyber criminals, they are certain to incur additional damages. Because identity thieves already have their PHI and PII, Plaintiffs and Class members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[28]

96. None of this should have happened. The Healthcare Data Breach was entirely preventable.

E. Defendant Could Have Prevented the Healthcare Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' PHI and PII

97. Data disclosures and data breaches are preventable.[29] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and

[28] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[29] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

implementation of appropriate security solutions."[30] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[31]

98. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[32]

99. Defendant required Plaintiffs and Class members to surrender their PHI and PII – including but not limited to their names, addresses, Social Security numbers, medical information, and health insurance information – and was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PHI and PII.

100. Defendant breached fiduciary duties owed to Plaintiffs and the Class as guardian of their PHI and PII.

101. Many failures laid the groundwork for the occurrence of the Healthcare Data Breach, starting with Defendant' failure to incur the costs necessary to implement adequate and reasonable cyber security training, procedures and protocols that were necessary to protect Plaintiffs' and Class members' PHI and PII.

102. Defendant maintained the PHI and PII in an objectively reckless manner, making the PHI and PII vulnerable to unauthorized disclosure.

103. Defendant knew, or reasonably should have known, of the importance of safeguarding PHI and PII and of the foreseeable consequences that would occur if Plaintiffs' and Class members' PHI and PII was stolen, including the significant costs that would be placed on

---

[30] *Id.* at 17.

[31] *Id.* at 28.

[32] *Id.*

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

Plaintiffs and Class members as a result of a breach.

104. The risk of improper disclosure of Plaintiffs' and Class members' PHI and PII was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class members' PHI and PII from that risk left the PHI and PII in a dangerous condition.

105. Defendant disregarded the rights of Plaintiffs and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the PHI and PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' PHI and PII; (iii) failing to take standard and reasonably available steps to prevent the Healthcare Data Breach; (iv) concealing the existence and extent of the Healthcare Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Healthcare Data Breach.

CLASS ACTION ALLEGATIONS

106. Plaintiffs bring this action under Federal Rule of Civil Procedure 23 against Defendant individually and on behalf of all others similarly situated. Plaintiffs assert all claims on behalf of the Class and Subclasses, defined as follows:

Nationwide Class

> All persons residing in the United States whose personal and/or medical information was compromised as a result of the Med-Data Healthcare Data Breach that occurred from sometime between December 2018 and September 2019 through December 17, 2020.

Missouri Subclass

> All persons residing in Missouri whose personal and/or medical information was compromised as a result of the Med-Data Healthcare Data Breach that occurred from sometime between December 2018 and September 2019 through December 17, 2020.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

107. Excluded from the Nationwide Class and Missouri Subclass are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

108. Plaintiffs reserve the right to amend the above definitions or to propose alternative or additional subclasses in subsequent pleadings and motions for class certification.

109. The Nationwide Class and Missouri Subclass are collectively referred to as the "Class" unless otherwise specified.

a. Class Certification is Appropriate

110. The proposed Class and Subclass meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

111. Numerosity: The proposed Class is believed to be so numerous that joinder of all members is impracticable. The proposed Subclasses are also believed to be so numerous that joinder of all members would be impractical.

112. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive PHI and PII compromised in the same way by the same conduct of Defendant.

113. Adequacy: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class and proposed Subclasses that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

114. Superiority: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

115. Commonality and Predominance: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's PHI and PII;

c. Whether Defendant's computer systems and data security practices used to protect Plaintiffs' and Class members' PHI and PII violated the FTC Act and/or HIPAA, and/or state laws and/or Defendant' other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PHI and PII, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach or disclosure;

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Healthcare Data Breach;

g. Whether Defendant breached contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PHI and PII;

h. Whether Defendant failed to adequately respond to the Healthcare Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

i. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

j. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief;

k. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and members of the Class;

l. Whether Defendant's actions and inactions alleged herein constitute gross negligence; and

m. Whether Plaintiffs and Class members are entitled to punitive damages.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of the Nationwide Class)

116. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

117. Defendant gathered and stored the PHI and PII of Plaintiffs and the Class as part of the operation of its business.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

118. Upon accepting and storing the PHI and PII of Plaintiffs and Class members, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods and to implement necessary data security protocols and employee training to do so.

119. Defendant had full knowledge of the sensitivity of the PHI and PII, the types of harm that Plaintiffs and Class members could and would suffer if the PHI and PII was wrongfully disclosed, and the importance of adequate security.

120. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their PHI and PII that was in Defendant' possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

121. Defendant owed Plaintiffs and Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing their PHI and PII, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

122. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

123. Defendant had duties to protect and safeguard the PHI and PII of Plaintiffs and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive PHI and PII. Additional duties that Defendant owed Plaintiffs and the Class include:

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' PHI and PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class members' PHI and PII in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiffs and Class members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PHI and PII.

124. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the PHI and PII that had been entrusted to them.

125. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class members' PHI and PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the PHI and PII in its possession;

b. Failing to protect the PHI and PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PHI and PII;

d. Failing to adequately train its employees to not store unencrypted PHI and PII in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's PHI and PII;

f. Failing to mitigate the harm caused to Plaintiffs and the Class members;

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiffs and Class members of the Healthcare Data Breach that affected their PHI and PII.

126. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

127. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

128. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PHI and PII of Plaintiffs and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PHI and PII of Plaintiffs and Class members while it was within Defendant's possession and control.

129. Further, through its failure to provide timely and clear notification of the Healthcare Data Breach to Plaintiffs and Class members, Defendant prevented Plaintiffs and Class members from taking meaningful, proactive steps to securing their PHI and PII and mitigating damages.

130. As a result of the Healthcare Data Breach, Plaintiffs and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Healthcare Data Breach on their lives, including but not limited to, paying for spyware removal, responding to the fraudulent use of the PHI and PII, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

131. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

132. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

133. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of the Nationwide Class)

134. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

135. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the PHI and PII of Plaintiffs and the Class.

136. Defendant is a covered entity under HIPAA, 45 C.F.R. §160.102, and as such is required to comply with the HIPAA's Privacy Rule and Security Rule. HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

137. HIPAA further requires Defendant to disclose the unauthorized access and theft of the protected health information of Plaintiffs and the Class "without unreasonable delay" so that Plaintiffs and Class members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their personal information. *See* 45 C.F.R. §§ 164.404, 164.406, and 164.410.

138. 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 Defendant,

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

of failing to use reasonable measures to protect PHI and PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

139. Defendant gathered and stored the PHI and PII of Plaintiffs and the Class as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

140. Defendant violated the FTC Act by failing to use reasonable measures to protect the PHI and PII of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

141. Defendant breached its duties to Plaintiffs and the Class under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class members' PHI and PII, and by failing to provide prompt notice without reasonable delay.

142. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

143. Plaintiffs and the Class are within the class of persons that HIPAA and the FTC Act were intended to protect.

144. The harm that occurred as a result of the Healthcare Data Breach is the type of harm HIPAA and the FTC Act were intended to guard against.

145. Defendant breached its duties to Plaintiffs and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PHI and PII.

146. Additionally, Defendant had a duty to promptly notify Plaintiffs and the Class of the Healthcare Data Breach. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Healthcare Data Breach. Defendant did not notify Plaintiffs or Class members of the Healthcare Data Breach until on or around March 31, 2021, despite knowing on or before December 10, 2020 that unauthorized persons had accessed and/or

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

viewed or were reasonably likely to have accessed and/or viewed private, protected, personal information of Plaintiffs and the Class.

147. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Healthcare Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

148. Defendant's violation of the FTC Act and HIPAA constitutes negligence *per se*.

149. As a direct and proximate result of Defendant' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Healthcare Data Breach, as alleged above.

150. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

151. Plaintiffs and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of the Nationwide Class)

152. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

153. Defendant entered into various written contracts with its clients, including AdventHealth Shawnee Mission, to perform services that include, but are not limited to, processing Medicaid eligibility, third-party liability, workers' compensation, and patient billing.

154. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Indeed, Defendant knew that if it were to breach these contracts with its clients, the clients' patients – Plaintiffs and Class members – would be harmed.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

155. Defendant breached the contracts it entered into with AdventHealth Shawnee Mission and its other clients by, among other things, failing to (i) use reasonable data security measures, and (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' PHI and PII from unauthorized disclosure to third parties.

156. As foreseen, Plaintiffs and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

157. Plaintiffs and Class members are also entitled to their costs and attorney's fees incurred in this action.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class)

158. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

159. Plaintiffs and Class members bring this cause of action alternatively to their claim for breach of third-party beneficiary contract.

160. Plaintiffs and Class members, as part of their agreements with Defendant, provided Defendant with their PHI and PII.

161. In providing such PHI and PII, Plaintiffs and Class members entered into implied contracts with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiffs' and Class members' PHI and PII.

162. Under the implied contracts, Defendant 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.

163. Defendant breached its implied contracts with Plaintiffs and Class members by failing to take reasonable measures to safeguard the PHI and PII.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

164. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class members' PHI and PII, Plaintiffs and 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, the untimely and/or inadequate notification of the Healthcare Data Breach, improper disclosure of their PHI and PII, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Healthcare Data Breach, the value of their time spent mitigating identity theft and/or identity fraud and/or increased risk of identity theft and/or identity fraud, and increased risk of identity theft and/or identity fraud.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of the Nationwide Class)

165. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

166. Plaintiffs and the Class bring this claim in the alternative to other claims and remedies at law.

167. Defendant, by way of its affirmative actions and omissions, including breaching its duties of care, was unjustly enriched by obtaining monetary benefits for the secure processing of patient's medical billings and claims while failing to reasonably secure Plaintiffs' and Class members' PHI and PII.

168. Plaintiffs and Class members suffered as a direct and proximate result of Defendant's failure to reasonably secure the PHI and PII entrusted to Defendant.

169. Accordingly, Plaintiffs and Class members are entitled to relief in the form of disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiffs and the Class.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

SIXTH CAUSE OF ACTION
NEGLIGENT TRAINING AND SUPERVISION
(On Behalf of the Nationwide Class)

170. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

171. At all times relevant hereto, Defendant owed a duty to Plaintiffs and the Class to hire competent employees and agents, and to train and supervise them to ensure that they recognize the duties owed to their patients and their parents.

172. Defendant breached the duty owed to Plaintiffs and the Class to supervise and train its employees by allowing its employees to give access to patient medical records to unauthorized users.

173. By posting Plaintiffs' and Class members' PHI and PII to the public-facing website, GitHub, Defendant's employee was clearly acting outside the scope of his/her employment and presented an extreme risk of harm to Plaintiffs and Class members.

174. Defendant knew, or in the exercise of reasonable care, should have known that the employee presented such a risk, but failed to take corrective action and adequately train and supervise the employee.

175. Defendant's failure to train and supervise the employee was the proximate cause of Plaintiffs' and Class members' injuries, as described herein.

176. As a direct result of Defendant's failure to train and supervise its employee, Plaintiffs and Class members 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, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Healthcare Data Breach, 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. At the very least, Plaintiffs and the other Class members are entitled to nominal damages.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

177. Defendant's wrongful actions and/or inaction and the resulting Healthcare Data Breach constituted (and continue to constitute) an invasion of Plaintiffs' and Class members' privacy by publicly and wrongfully permitting the disclosure of Plaintiffs' and Class members PHI and PII without their authorization or consent. This unauthorized disclosure was a direct result of Defendant's negligent training and supervision of its employees.

SEVENTH CAUSE OF ACTION
INVASION OF PRIVACY (INTRUSION UPON SECLUSION)
(On Behalf of the Nationwide Class)

178. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

179. Plaintiffs and Class members reasonably expected that the sensitive PHI and PII entrusted to Defendant would be kept private and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

180. Defendant unlawfully invaded the privacy rights of Plaintiffs and Class members by:

a. Failing to adequately secure their sensitive PHI and PII from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of personal and sensitive facts and information about them in a manner highly offensive to a reasonable person; and

c. Enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

181. A reasonable person would find it highly offensive that Defendant, having collected Plaintiffs' and Class members' sensitive PHI and PII, failed to protect such PHI and PII from unauthorized disclosure to third parties.

182. Indeed, such disclosure goes against the public policies of the State of Washington. For example, RCW 70.02.005 provides: "Persons other than health care providers obtain, use, and disclose health record information in many different contexts and for many

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

different purposes. It is the public policy of this state that a patient's interest in the proper use and disclosure of the patient's health care information survives even when the information is held by persons other than health care providers."

183. In failing to adequately protect Plaintiffs' and Class members' sensitive personal information, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that its ineffective security measures, and the foreseeable consequences thereof, are highly offensive to a reasonable person in Plaintiffs' and Class members' position.

184. Defendant violated Plaintiffs' and Class members' right to privacy under the common law.

185. Defendant's unlawful invasions of privacy damaged Plaintiffs and the Class. As a direct and proximate result of Defendant's unlawful invasion of privacy, Plaintiffs and Class members suffered significant anxiety and distress, and their reasonable expectations of privacy were frustrated and defeated. Plaintiffs and the Class seek actual and nominal damages for these invasions of privacy.

EIGHTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY
(On Behalf of the Nationwide Class)

186. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

187. At all relevant times hereto, Defendant owed, and owes, a fiduciary duty to Plaintiffs and the Class to keep Plaintiffs' PHI and PII.

188. The fiduciary duty of privacy is explicated under the procedures set forth in RCW 70.02.270, which required Defendant to secure the health care information it maintains and to keep it free from disclosure.

189. Defendant breached its fiduciary duty to Plaintiff by disclosing Plaintiffs' and other Class members' PHI and PII to unauthorized third parties.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

190. As a direct result of Defendant's breach of its fiduciary duty of confidentiality and the disclosure of Plaintiffs' confidential PHI and PII, Plaintiffs and the Class members have suffered damages.

191. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class members' PHI and PII, Plaintiffs and the Class have 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, and humiliation.

192. 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 the 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 Class are entitled to nominal damages.

NINTH CAUSE OF ACTION
VIOLATION OF WASHINGTON CONSUMER PROTECTION ACT,
RCW 19.86, *ET SEQ.*
(On Behalf of the Nationwide Class)

193. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

194. Defendant is a "person" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010 and it conducts "trade" and "commerce" within the meaning of RCW 19.86.010(2).

195. Plaintiffs and the Class are "persons" within the meaning of RCW 19.86.010(1).

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

196. Defendant engaged in unfair or deceptive acts or practices in the conduct of its business by through the conduct set forth throughout this Complaint. These unfair or deceptive acts or practices include, without limitation, the following:

a. Failing to adequately secure Plaintiffs' and Class members' PHI and PII from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of Plaintiffs' and Class members' PHI and PII in a manner highly offensive to a reasonable person;

c. Enabling the disclosure of Plaintiffs' and Class members' PHI and PII without their informed, voluntary, affirmative, and clear consent;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PHI and PII; and

e. Failing to disclose the Healthcare Data Breach in a timely and accurate manner.

197. Defendant's systematic acts or practices are unfair because these acts or practices (1) caused substantial financial injury to Plaintiffs' and Class members; (2) are not outweighed by any countervailing benefits to consumers or competitors; and (3) are not reasonably avoidable by consumers.

198. Defendant's systematic acts or practices are unfair because the acts or practices are immoral, unethical, oppressive, and/or unscrupulous.

199. Defendant's systematic acts or practices are deceptive because they were, and are capable of, deceiving a substantial portion of the public.

200. Defendant's unfair and deceptive acts or practices have repeatedly occurred in trade or commerce within the meaning of RCW 19.86.010 and RCW 19.86.020.

201. The acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

202. Defendant's unfair or deceptive acts or practices impact the public interest because they have injured Plaintiffs and Class members.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

203. As a direct and proximate result of Defendant's unfair or deceptive acts or practices, Plaintiffs and Class members have suffered injury in fact and lost money.

204. As a result of Defendant's conduct, Plaintiffs and Class members have suffered actual damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased and imminent risk of fraud and identity theft, the lost value of their PHI and PII, and other economic and non-economic harm.

205. Plaintiffs and the Class are therefore entitled to legal relief against Defendant, including recovery of nominal damages, actual damages, treble damages, injunctive relief, attorneys' fees and costs, and such further relief as the Court may deem proper.

206. Plaintiffs and the Class are also entitled to injunctive relief in the form of an order prohibiting Defendant from engaging in the alleged misconduct and such other equitable relief as the Court deems appropriate.

TENTH CAUSE OF ACTION
VIOLATIONS OF MISSOURI MERCHANDISING PRACTICES ACT ("MMPA")
MO. REV. STAT. § 407.010 ET SEQ.
(On Behalf of the Missouri Subclass)

207. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

208. 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…"

209. An "unfair practice" is defined by Missouri law 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 decision; or

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers. *See* 15 CSR 60-8.020.

210. An "unfair practice" is also defined as "an 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*" (emphasis added); *see* 15 CSR 60-8.040.

211. Plaintiffs and Defendant are "persons" within the meaning of Section 407.010(5).

212. "Merchandise" is defined by the MMPA to include providing "services" and, therefore, encompasses healthcare services. Healthcare services are a "good."

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

214. Maintenance of medical records is "merchandise" within the meaning of section 407.010(4).

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

216. As set forth herein, Defendant's acts, practices and conduct violate Section 407.010(i) in that, among other things, Defendant has 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 offend the public policy established by Missouri statute and constitute an "unfair practice" as that term is used in Section 407.020(1).

217. Defendant's unfair, unlawful and deceptive acts, practices and conduct include the following: (i) representing to its patients that it would not disclose their sensitive personal health information to an unauthorized third party or parties; (ii) failing to implement proper

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

security measures such as securing the records in a safe place; and (3) failing to adequately train its personnel.

218. Defendant's conduct also violates the enabling regulations for the MMPA because it (i) offends public policy; (ii) is unethical, oppressive and unscrupulous; (iii) causes substantial injury to consumers; (iv) is not in good faith; (v) is unconscionable; and (vi) is unlawful. *See* Mo. Code Regs. Ann. tit. 15, Section 60-8.

219. As a direct and proximate cause of Defendant's unfair and deceptive acts, Plaintiffs and members of the Class have suffered damages in that they (i) paid more for medical record privacy protections than they otherwise would have, and (ii) 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.

220. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class members' PHI and PII, Plaintiffs and Class members 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, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Healthcare Data Breach, 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.

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

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

ELEVENTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of the Nationwide Class)

222. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

223. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

224. As previously alleged, Plaintiffs and members of the Class entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the PHI and PII it collected from Plaintiffs and the Class.

225. Defendant owes a duty of care to Plaintiffs and Class members that require it to adequately secure Plaintiffs' and Class members' PHI and PII.

226. Defendant still possesses the PHI and PII of Plaintiffs and the Class members.

227. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class members.

228. Actual harm has arisen in the wake of the Healthcare Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and the members of the Class. Further, Plaintiffs and the members of the Class are at risk of additional or further harm due to the exposure of their PHI and PII and Defendant's failure to address the security failings that led to such exposure.

229. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

230. Plaintiffs and the Class, therefore, seek a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant provide employee training regarding the dangers and risks inherent in using file-sharing websites like the Website at issue here to store and/or transmit PHI and PII;

e. Ordering that Defendant cease transmitting PHI and PII via file-sharing websites like the Website at issue here;

f. Ordering that Defendant cease storing PHI and PII on file-sharing websites like the Website at issue here;

g. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any PHI and PII not necessary for its provision of services;

h. Ordering that Defendant conduct regular database scanning and security checks; and

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

not limited to, patient personally identifiable information and patient protected health information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Class Action Complaint.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

Dated: August 9, 2021.

s/Matthew J. Ide, WSBA No. 26002
Matthew J. Ide, WSBA No. 26002
IDE LAW OFFICE
7900 SE 28th Street, Suite 500
Mercer Island, WA 98040
Tel. (206) 625-1326
Fax: (206) 622-0909
email: mjide@yahoo.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

Maureen M. Brady*
MCSHANE & BRADY, LLC
1656 Washington Street, Suite 120
Kansas City, MO 64108
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
mbrady@mcshanebradylaw.com

**pro hac vice* admission request forthcoming

Counsel for Plaintiffs and the Putative Class