UNITED STATES DISTRICT COURT

DISTRICT OF CONNECTICUT

JESSICA GUERRERO, JEFFREY MATTHEWS and JOSEPH CASTILLO, individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

MERRITT HEALTHCARE HOLDINGS, LLC d/b/a MERRITT HEALTHCARE ADVISORS,

Defendant.

Case No. 3:23-cv-00389-MPS

CLASS ACTION

CONSOLIDATED AMENDED COMPLAINT

JURY TRIAL DEMANDED

July 26, 2023

Representative Plaintiffs allege as follows:

INTRODUCTION

1. Representative Plaintiffs Jessica Guerrero, Jeffrey Matthews, and Joseph Castillo ("Representative Plaintiffs") bring this Consolidated Amended Class Action Complaint against Defendant Merritt Healthcare Holdings, LLC d/b/a Merritt Healthcare Advisors ("Defendant" or "Merritt") for its failure to properly secure and safeguard Representative Plaintiffs' and Class Members' protected health information and personally identifiable information stored within Defendant's information network, including, without limitation, full names, treatment information, provider names, patient identification numbers, health insurance information, treatment cost information, and health insurance numbers (these types of information, *inter alia*, being thereafter

referred to, collectively, as "protected health information" or "PHI"[1] and "personally identifiable information" or "PII").[2]

2. With this action, Representative Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiffs and, at least, 77,258[3] other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on November 30, 2022, in which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PHI/PII that was being kept unprotected ("Data Breach").

3. Representative Plaintiffs further seek to hold Defendant responsible for not ensuring that PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164), and other relevant standards.

4. While Defendant claims to have discovered the breach as early as November 30, 2022, Defendant did not inform victims of the Data Breach until March 14, 2023. Indeed, Representative Plaintiffs and Class Members were wholly unaware of the Data Breach until they received letters from Defendant informing them of it.

---

[1] Protected health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

[3] *Breach Portal*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf/ (last accessed April 12, 2023).

5. Defendant acquired, collected, and stored Representative Plaintiffs' and Class Members' PHI/PII. Therefore, at all relevant times, Defendant knew or should have known that Representative Plaintiffs and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PHI/PII.

6. HIPAA establishes national minimum standards for protecting individuals' medical records and other protected health information. HIPAA, generally, applies to health plans/insurers, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically and sets minimum standards for Defendant's maintenance of Representative Plaintiffs' and Class Members' PHI/PII. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Representative Plaintiffs' and Class Members' PHI/PII, including rights to examine and obtain copies of their health records and to request corrections thereto.

7. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

8. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiffs' and Class Members' PHI/PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from HIPAA, other state and federal statutes and regulations, and common law principles. Representative Plaintiffs do not bring claims in this action for direct

violations of HIPAA but charge Defendant with various legal violations merely predicated upon the duties set forth in HIPAA.

9. Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' PHI/PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiffs' and Class Members' PHI/PII was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant.

11. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

12. Defendant is headquartered and/or routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State, has intentionally availed itself

of this jurisdiction by marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within this State.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiffs' claims took place within this District and Defendant is headquartered and/or does business in this Judicial District.

REPRESENTATIVE PLAINTIFFS' COMMON EXPERIENCES

14. Defendant received highly sensitive PHI/PII from Representative Plaintiffs in connection with the services and/or employment Representative Plaintiffs received or requested. As a result, Representative Plaintiffs' information was among the data an unauthorized third party accessed in the Data Breach.

15. Representative Plaintiffs were and are very careful about sharing their PHI/PII. Representative Plaintiffs have never knowingly transmitted unencrypted sensitive PHI/PII over the internet or any other unsecured source.

16. Representative Plaintiffs stored any documents containing their PHI/PII in a safe and secure location or destroyed the documents. Moreover, Representative Plaintiffs diligently chose unique usernames and passwords for their various online accounts.

17. Representative Plaintiffs took reasonable steps to maintain the confidentiality of their PHI/PII and relied on Defendant to keep their PHI/PII confidential and securely maintained, to use this information for employment purposes only, and to make only authorized disclosures of this information.

18. The Notice from Defendant (the website version of this Notice, which is substantially similar in content to the Notices received by Representative Plaintiffs and the Class,

is attached as **Exhibit A**) notified Representative Plaintiffs that Defendant's network had been accessed and that Plaintiffs' PHI/PII may have been involved in the Data Breach.

19. Furthermore, Defendant's Notice directed Representative Plaintiffs to be vigilant and to take certain steps to protect their PHI/PII and otherwise mitigate their damages.

20. As a result of the Data Breach, Plaintiffs heeded Defendant's warnings and spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice and self-monitoring their accounts and credit reports to ensure no fraudulent activity had occurred. This time has been lost forever and cannot be recaptured.

21. Representative Plaintiffs suffered actual injury in the form of damages to and diminution in the value of Representative Plaintiffs' PHI/PII—a form of intangible property that Representative Plaintiffs entrusted to Defendant, which was compromised in and because of the Data Breach.

22. Representative Plaintiffs suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and have anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling Representative Plaintiffs' PHI/PII.

23. Representative Plaintiffs suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PHI/PII, in combination with their names, being placed in the hands of unauthorized third parties/criminals.

24. Representative Plaintiffs have a continuing interest in ensuring that Representative Plaintiffs' PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Jessica Guerrero's Experiences

25. On or about March 14, 2023, Representative Plaintiff Guerrero was notified via letter from Defendant that her PHI and/or PII had been accessed because of the Data Breach.

26. Representative Plaintiff Guerrero is an adult individual and, at all times relevant herein, a resident and citizen of the State of Virginia. Representative Plaintiff Guerrero is a victim of the Data Breach. Defendant received Representative Plaintiff Guerrero's PHI/PII in connection with the services she received at the Delaware Surgery Center, a client of Defendant's.

27. Plaintiff Guerrero last visited the Delaware Surgery Center in June of 2019 and was unaware that Defendant obtained or retained her PHI/PII.

28. As a result, Representative Plaintiff Guerrero's information was among the data an unauthorized third party accessed in the Data Breach.

29. Since the Data Breach, Plaintiff Guerrero has experienced an uptake in spam calls concerning fraudulent applications/solicitations for insurance, fraudulent communications about her FICO score or FHA loans, fraudulent communications from her "bank," and at least one instance in which an unauthorized third party redirected a package ordered by Plaintiff Guerrero on Amazon to an unknown address in Chicago.

30. Plaintiff Guerrero also received a bill from SeaWorld in her name that she did not incur, which she is investigating as fraudulent.

31. Plaintiff Guerrero monitors her credit and identity for fraudulent activity every day since the Breach, for at least a couple hours a day.

32. Plaintiff Guerrero is made uncomfortable because her personal information and all of her health information are out there and is particularly concerned that her children's information may be out there as well.

Plaintiff Jeffrey Matthews' Experiences

33. On or about March 14, 2023, Representative Plaintiff Matthews was notified via letter from Defendant that his PHI and/or PII had been accessed because of the Data Breach.

34. Representative Plaintiff Matthews is an adult individual and, at all times relevant herein, a resident and citizen of the State of Kansas. Representative Plaintiff Matthews is a victim of the Data Breach. Defendant received Representative Plaintiff Matthews' PHI/PII in connection with the services Representative Plaintiff Matthews received from Defendant. As a result, Representative Plaintiff Matthews' information was among the data an unauthorized third party accessed in the Data Breach.

Plaintiff Joseph Castillo's Experiences

35. On or about March 20, 2023, Representative Plaintiff Castillo was notified via letter from Defendant that his PHI and/or PII had been accessed because of the Data Breach.

36. Representative Plaintiff Castillo is an adult individual and, at all times relevant herein, a resident and citizen of the State of California. Representative Plaintiff Castillo is a victim of the Data Breach. Defendant received Representative Plaintiff Castillo's PHI/PII in connection with the services he received from a healthcare provider affiliated with Defendant. Representative Plaintiff Castillo provided further information to Defendant due to his employment with Bakersfield Heart Hospital, a healthcare provider affiliated with Defendant from 2013 through 2019. Representative Plaintiff Castillo's information was among the data an unauthorized third party accessed in the Data Breach. The Notice Representative Plaintiff Castillo received does not explain which parts of his PHI and/or PII were taken, but instead generically states that the files contained his PHI and PII "including [his] name and Social Security Number." *See* **Exhibit A** (stating same).

37. Representative Plaintiff Castillo is especially alarmed by the vagueness of this Notice, as he cannot tell what information was taken in the Breach. Moreover, he is very disturbed by the fact that his Social Security number was identified as among the breached data on Defendant's computer system.

38. Representative Plaintiff Castillo has already been receiving alerts to change his passwords as they were found on the dark web. He plans to change his passwords and freeze his credit to mitigate identity fraud risks.

39. As of a few months ago, Representative Plaintiff Castillo began receiving an excessive number of spam calls on the same cell phone number he used while engaging with Defendant. Moreover, he receives many spam emails and texts now, which was not typical before the Data Breach. Representative Plaintiff Castillo believes the Data Breach caused these spam messages.

40. On July 11, 2023, Representative Plaintiff Castillo sent a notice letter to Merritt Healthcare Advisors pursuant to the California Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code § 1750, and the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.100, *et seq*. To date, Merritt has not responded to Representative Plaintiff Castillo's demands.

DEFENDANT

41. Defendant Merritt Healthcare Holdings, LLC d/b/a Merritt Healthcare Advisors is a Delaware limited liability corporation with a principal place of business located at 75 Danbury Road, Unit B5, Copps Hill Court, Ridgefield, Connecticut 06877.

42. Defendant develops and manages ambulatory surgery centers nationwide. Per Defendant's website, it "develop[s] facilities where procedures are performed safely, efficiently

and in a cost-effective manner."[4] It "represent[s] healthcare business owners throughout the United States who are considering a strategic and/or financial transaction."[5]

43. According to its website, Defendant "was founded with the sole purpose of representing owners of healthcare organizations who would benefit significantly from our representation during a transaction with a hospital, healthcare system, national or regional strategic company, private equity or any of the prospective buyers and partners in their businesses."[6]

44. Defendant claims to be an industry leader who has used its healthcare advisory experience to "successfully complete more than $4 billion in transactions on behalf of [its] Clients."[7]

45. Defendant is a business associate with its covered entity subsidiaries such as Bakersfield Heart Hospital, Kansas Spine and Specialty Hospital, Forest Surgery Center, and Delaware Surgery Center. **Exhibit A.**

46. Defendant has one member who is a resident and citizen of Connecticut, with its principal business and residence address at 75 Danbury Road, Unit B5. Copps Hill Courts, Ridgefield, Connecticut 06877. Its registered agent, United States Corporation Agents, Inc., can be served at 651 N. Broad Street, Suite 201, Middletown, Delaware 19709.

47. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

---

4 *About Us*, https://merritthealthcare.com/about-us/ (last accessed April 12, 2023).
5 *Who We Serve,* https://merrittadvisory.com/who-we-serve/ (last accessed April 18, 2023).
6 *Who We Serve,* https://merrittadvisory.com/who-we-serve/ (last accessed April 18, 2023).
7 *Merritt Investment Banking,* https://merrittadvisory.com/ (last accessed April 18, 2023).

CLASS ACTION ALLEGATIONS

48. Representative Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure ("F.R.C.P.") on behalf of Representative Plaintiffs and the following classes/subclass(es) (collectively, the "Class(es)"):

> **Nationwide Class:**
> "All individuals within the United States of America whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on November 30, 2022."
>
> **California Subclass:**
> "All individuals within the State of California whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on November 30, 2022."
>
> **Virginia Subclass:**
> "All individuals within the State of Virginia whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on November 30, 2022."
>
> **Kansas Subclass:**
> "All individuals within the State of Kansas whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on November 30, 2022."

49. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

50. In the alternative, Representative Plaintiffs request additional subclasses as necessary based on the types of PHI/PII that were compromised.

51. Representative Plaintiffs reserve the right to amend the above Class definitions or to propose other subclasses in subsequent pleadings and motions for class certification.

52. This action has been brought and may properly be maintained as a class action under F.R.C.P. Rule 23 because there is a well-defined community of interest in the litigation and membership of the proposed Classes is readily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiffs are informed and believe and, on that basis, allege that the total number of Class Members is in the thousands of individuals. Membership in the Classes will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiffs and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiffs and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiffs and Class Members that their PHI/PII had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PHI/PII of Representative Plaintiffs and Class Members;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiffs' and Class Members' PHI/PII;

11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

12) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiffs' claims are typical of the claims of the Plaintiff Classes. Representative Plaintiffs and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiffs in this class action are adequate representatives of each of the Plaintiff Classes in that Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to the vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in their entirety. Representative Plaintiffs anticipate no management difficulties in this litigation.

e. Superiority of Class Action: The damages suffered by individual Class Members are significant but may be small relative to each member's enormous expense of individual litigation. This makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately. Individualized litigation increases the delay and expense to all parties and to the court system, presented by the case's complex legal and factual issues. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court.

53. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, so it is impracticable to bring all Class Members before the Court.

54. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Classes in their entireties. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly. Representative Plaintiffs' challenge of these policies and procedures hinges on Defendant's conduct concerning the Classes in their entirety, not on facts or law applicable only to Representative Plaintiff.

55. Unless a Class-wide injunction is issued, Defendant may continue failing to secure Class Members' PHI/PII properly, and Defendant may continue to act unlawfully, as set forth in this Complaint.

56. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under F.R.C.P. Rule 23(b)(2).

COMMON FACTUAL ALLEGATIONS

The Data Breach

57. During the Data Breach, one or more unauthorized third parties accessed Class Members' sensitive data including, but not limited to full names, treatment information, provider names, patient identification numbers, health insurance information, treatment cost information, and health insurance numbers. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

58. According to Defendant, the Data Breach occurred when an actor gained "unauthorized access to one Merritt employee's email account." **Exhibit A.**

59. According to the Data Breach Notification, which Defendant filed with the United States Department of Health and Human Services, 77,258 persons were affected.[8]

60. Representative Plaintiffs were provided the information detailed above upon Representative Plaintiffs' receipt of a Defendant's Notice. Representative Plaintiffs were not aware of the Data Breach until receiving this letter.

61. According to the undated "Notice of Data Security Incident" that Defendant posted on its website, "[a]fter an extensive forensic investigation and manual document review, Merritt discovered on November 30, 2022 that some personal information was contained in the account that was accessed between July 30, 2022 and August 25, 2022." **Exhibit A.**

62. In other words, an unauthorized actor had access to the employee account for almost an entire month without the account being secured or the Breach being discovered.

63. However, without further explanation, in its website notice letter, Defendant claims that it "is committed to maintaining the privacy of personal information in its possession and has taken additional precautions to safeguard it." **Exhibit A.** It claims it "notified individuals whose information was included in the accessed account. Notified individuals have been provided with best practices to protect their information, including placing a fraud alert and/or security freeze on their credit files and obtaining a free credit report." **Exhibit A.**

Defendant's Failed Response to the Data Breach

64. Not until roughly four months after it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PHI/PII Defendant confirmed was

[8] *Breach Portal*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed April 12, 2023).

potentially compromised because of the Data Breach. The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

65. The Notice included, *inter alia*, the claims that Defendant had learned of the Data Breach on November 30, 2022, and had taken steps to respond. But the Notice lacked sufficient information on how the breach occurred, what safeguards have been taken since then to safeguard further attacks, and/or where the information hacked exists today.

66. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' PHI/PII with the intent of misusing the PHI/PII, including marketing and selling Representative Plaintiffs' and Class Members' PHI/PII.

67. Defendant had and continues to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Representative Plaintiffs' and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

68. Representative Plaintiffs and Class Members were required to provide their PHI/PII to Defendant to receive healthcare, and as part of providing healthcare Defendant created, collected, and stored Representative Plaintiffs' and Class Members' PHI/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.

69. Despite this, even today, Representative Plaintiffs and Class Members remain in the dark regarding what data was stolen, the particular malware used, and what steps are being taken to secure their PHI/PII in the future. Thus, Representative Plaintiffs and Class Members are left to speculate as to where their PHI/PII ended up, who has used it, and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach

and how Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

70. Representative Plaintiffs' and Class Members' PHI/PII may end up for sale on the dark web or fall into the hands of companies that will use the detailed PHI/PII for targeted marketing without Representative Plaintiffs' and/or Class Members' approval. Either way, unauthorized individuals can now easily access Representative Plaintiffs' and Class Members' PHI/PII.

Defendant Collected/Stored Representative Plaintiffs' and Class Members' PHI/PII

71. Defendant acquired, collected, stored, and assured reasonable security over Representative Plaintiffs' and Class Members' PHI/PII.

72. As a condition of its relationships with Representative Plaintiffs and Class Members, Defendant required that Representative Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential PHI/PII. Defendant, in turn, stored that information on Defendant's system that was ultimately affected by the Data Breach.

73. By obtaining, collecting, and storing Representative Plaintiffs' and Class Members' PHI/PII, Defendant assumed legal and equitable duties over the PHI/PII and knew or should have known that it was thereafter responsible for protecting Representative Plaintiffs' and Class Members' PHI/PII from unauthorized disclosure.

74. Representative Plaintiffs and Class Members have taken reasonable steps to maintain their PHI/PII's confidentiality. Representative Plaintiffs and Class Members relied on Defendant to keep their PHI/PII confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

75. Defendant could have prevented the Data Breach, which began as early as July 2022, by properly securing and encrypting and/or more securely encrypting its servers, generally, as well as Representative Plaintiffs' and Class Members' PHI/PII.

76. Defendant's negligence in safeguarding Representative Plaintiffs' and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed at protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

77. The healthcare industry has experienced many high-profile cyberattacks in the last several years preceding this Complaint's filing. Cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[9] According to the HIPAA Journal, the largest healthcare data breaches were reported in April 2021.[10]

78. For example, Universal Health Services experienced a cyberattack on September 29, 2020 similar to the attack on Defendant. As a result of this attack, Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[11] Similarly, in 2021, Scripps Health suffered a cyberattack, which effectively shut down critical healthcare services for a month and left numerous patients unable to speak to their physicians or access vital medical and prescription records.[12] University of San Diego Health suffered a similar attack a few months later.[13]

---

[9] https://www.hipaajournal.com/2020-healthcare-data-breach-report/ (last accessed July 24, 2023).

[10] https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last accessed July 24, 2023).

[11] https://www.prnewswire.com/news-releases/universal-health-services-inc-reports-2020-fourth-quarter-and-full-year-financial-results-and-2021-full-year-earnings-guidance-301236075.html/ (last accessed July 24, 2023).

[12] https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/ (last accessed July 24, 2023).

[13] https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/ (last accessed July 24, 2023).

79. 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."[14]

80. The HIPAA Journal article explains that patient records, like those stolen from Defendant, are "often processed and packaged with other illegally obtained data to create full record sets (full) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals, which "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."[15]

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

82. Due to the high-profile nature of these breaches and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack.

83. And yet, despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' PHI/PII from being compromised.

---

[14] *Editorial: Why Do Criminals Target Medical Records,* HIPAA J. (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/

[15] *Id.*

Defendant Had a Duty to Protect the Stolen Information

84. In failing to adequately secure Representative Plaintiffs' and Class Members' sensitive data, Defendant breached duties it owed Representative Plaintiffs and Class Members under statutory and common law. Under HIPAA, health insurance providers and business associates have an affirmative duty to keep patients' protected health information private. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiffs' and Class Members' data. Moreover, Representative Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also had an implied duty to safeguard their data, independent of any statute.

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

86. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for protecting health information.

87. 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.

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

89. "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.

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

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

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

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

d. Ensure compliance by its workforce.

91. 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" under 45 C.F.R. § 164.306(e), and 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).

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

93. 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 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).

94. According to the FTC, the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PHI/PII.

95. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that companies should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of PHI/PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

96. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

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

98. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

99. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PHI/PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

100. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Representative 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 Representative Plaintiffs' and Class Members' PHI/PII.

101. Defendant owed a duty to Representative Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that all PHI/PII in its possession was adequately secured and protected.

102. Defendant owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect all PHI/PII in its possession, including not sharing information with other entities who maintain sub-standard data security systems.

103. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach of its data security systems in a timely manner.

104. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

105. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft, because such an inadequacy would be a material fact in the decision to entrust this PHI/PII to Defendant.

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

107. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity to identify possible threats.

The Sensitive Information Stolen in the Data Breach is Highly Valuable

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

109. Individuals place a high value not only on their PHI/PII but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight the impact of identity theft.

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

111. The high value of PHI/PII to criminals is evidenced by the prices they will pay for it through the dark web. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[16] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[17] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[18]

112. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[19] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[20] In short, these sorts of data breaches are

[16] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 24, 2023).
[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 24, 2023).
[18] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 24, 2023).
[19] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed July 24, 2023).
[20] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed July 24, 2023).

increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[21]

113. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiff and Class Members. For example, it is believed that certain PHI/PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

114. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

115. Identity thieves can use PHI/PII, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate various crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

[21] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/ (last accessed July 24, 2023).

116. The ramifications of Defendant's failure to secure Representative Plaintiffs' and Class Members' PHI/PII are long-lasting and severe. Once PHI/PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PHI/PII of Representative Plaintiffs and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PHI/PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

118. 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, Representative Plaintiffs and Class Members cannot obtain new numbers unless they become victims of Social Security misuse.

119. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[22]

[22] *Identity Theft and Your Social Security Number*, SSA, No. 05-10064 (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 18, 2023).

120. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII 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.[23]

121. The harm to Representative Plaintiffs and Class Members is especially acute given the nature of the leaked data. 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," more than identity thefts involving banking and finance, the government, and the military or education.[24]

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

123. When cybercriminals access financial information, health insurance information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiffs and Class Members.

124. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-

---

[23] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed July 24, 2023).
[24] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed July 24, 2023).
[25] *Id*.

pocket costs for healthcare they did not receive to restore coverage.[26] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[27]

125. And data breaches are preventable.[28] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[29] 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…."[30]

126. 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 rigorously and disciplined so that a *data breach never occurs*.[31]

127. Here, Defendant knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Representative Plaintiffs' and Class Members' PHI/PII was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members because of a breach of this magnitude. As detailed above, Defendant

---

[26] See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed July 24, 2023).
[27] 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/ (last accessed July 24, 2023).
[28] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[29] *Id.* at 17.
[30] *Id.* at 28.
[31] *Id.*

knew or should have known that the development and use of such protocols was necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Therefore, its failure to do so is intentional, willful, reckless, and/or grossly negligent.

128. Furthermore, Defendant has offered only a limited one-year subscription for identity theft monitoring and identity theft protection through IDX. Its limitation is inadequate when the victims will likely face many years of identity theft.

129. Moreover, Defendant's credit monitoring offer and advice to Representative Plaintiffs and Class Members squarely place the burden on Representative Plaintiffs and Class Members, rather than on Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Representative Plaintiffs and Class Members to protect themselves from its tortious acts resulting from the Data Breach. Rather than automatically enrolling Representative Plaintiffs and Class Members in credit monitoring services upon discovery of the Data Breach, Defendant merely sent instructions to Representative Plaintiffs and Class Members about actions they could affirmatively take to protect themselves.

130. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Representative Plaintiffs' and Class Members' PHI/PII.

131. Defendant disregarded the rights of Representative Plaintiffs and Class Members by, *inter alia*: (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequate security protocols and training practices in place to safeguard Representative Plaintiffs' and Class Members' PHI/PII, (iii) failing

to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

CAUSES OF ACTION

COUNT ONE
Negligence
(On behalf of the Nationwide Class)

132. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

133. At all times herein relevant, Defendant owed Representative Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Representative Plaintiffs' and Class Members' PHI/PII on its computer systems and networks.

134. Among these duties, Defendant was expected:

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

b. to protect Representative Plaintiffs' and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to act on warnings about data breaches timely; and

d. to promptly notify Representative Plaintiffs and Class Members of any data breach, security incident or intrusion that affected or may have affected their PHI/PII.

135. Defendant knew or should have known that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty

of care to not subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

136. Defendant knew or should have known of the risks inherent in collecting and storing PHI/PII, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches.

137. Defendant knew or should have known that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' PHI/PII.

138. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PHI/PII that Representative Plaintiffs and Class Members had entrusted to it.

139. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PHI/PII.

140. Because Defendant knew that a breach of its systems could damage numerous individuals, including Representative Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PHI/PII stored thereon.

141. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with their PHI/PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant could protect its systems and the PHI/PII it stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiffs and Class Members.

142. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' PHI/PII and

promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Representative Plaintiffs, and/or the remaining Class Members.

143. Defendant breached its general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable and/or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' PHI/PII;

b. by failing to timely and accurately disclose that Representative Plaintiffs' and Class Members' PHI/PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard PHI/PII by knowingly disregarding standard information security principles, despite obvious risks and by allowing unmonitored and unrestricted access to unsecured PHI/PII;

d. by failing to provide adequate supervision and oversight of the PHI/PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Representative Plaintiffs' and Class Members' PHI/PII, misuse the PHI/PII and intentionally disclose it to others without consent;

e. by failing to adequately train its employees not to store ger than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiffs' and Class Members' PHI/PII;

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

h. by failing to encrypt Representative Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

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

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

146. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI/PII to Representative Plaintiffs and Class Members so

that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PHI/PII.

147. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting roughly four months after learning of the Data Breach to notify Representative Plaintiffs and Class Members and then by failing and continuing to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiffs and Class Members.

148. Further, explicitly failing to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendant prevented Representative Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PHI/PII and access their medical records and histories.

149. There is a close causal connection between Defendant's failure to implement security measures to protect Representative Plaintiffs' and Class Members' PHI/PII and the harm (or risk of imminent harm suffered) by Representative Plaintiffs and Class Members. Representative Plaintiffs' and Class Members' PHI/PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing and maintaining appropriate security measures.

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

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

152. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) 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, of failing to use reasonable measures to protect PHI/PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

153. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PHI/PII and by not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiff and Class Members.

154. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se.* Defendant also violated the HIPAA Privacy and Security rules, which constitutes negligence *per se*.

155. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PHI/PII is used, (iii) the compromise, publication, and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to

prevent, detect, contest, and recover from embarrassment and identity theft, (vi) lost continuity in relation to their healthcare, (vii) the continued risk to their PHI/PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' PHI/PII in its continued possession, and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

156. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members 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.

157. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer the continued risks of exposure of their PHI/PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PHI/PII in its continued possession.

COUNT TWO
Negligence *Per Se*
(On behalf of the Nationwide Class)

158. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

159. HIPAA requires that covered entities and business associates "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected

health information" and "must reasonably safeguard protected health information from any intentional or unintentional use or disclosure…." 45 CFR § 164.530I.

160. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 requires HIPAA covered entities and their business associates to provide notification to the United States Department of Health and Human Services, prominent media outlets following a data breach or any breach of unsecured protected health information without unreasonable delay and in no event later than 60 days after discovery of a data breach.

161. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits companies such as Defendant from "using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce," including failing to use reasonable measures to protect PHI/PII. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

162. In addition to the FTC rules and regulations and state law, other states and jurisdictions where victims of the Data Breach are located require that Defendant protect PHI/PII from unauthorized access and disclosure and timely notify the victim of a data breach.

163. Defendant violated HIPAA and FTC rules and regulations obligating companies to use reasonable measures to protect PHI/PII by failing to comply with applicable industry standards and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of a Data Breach and the exposure of Representative Plaintiffs' and Class members' highly sensitive PHI/PII.

164. Each of Defendant's statutory violations of HIPAA, Section 5 of the FTC Act and other applicable statutes, rules and regulations, constitute negligence *per se*.

165. Representative Plaintiffs and Class Members are within the category of persons HIPAA and the FTC Act were intended to protect.

166. The harm that occurred because of the Data Breach described herein is the type of harm HIPAA and the FTC Act were intended to guard against.

167. As a direct and proximate result of Defendant's negligence *per se*, Representative Plaintiffs and Class Members have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PHI/PII in Defendant's possession and are entitled to damages in an amount to be proven at trial.

COUNT THREE
Breach of Confidence
(On behalf of the Nationwide Class)

168. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

169. During Representative Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential nature of the PHI/PII that Representative Plaintiffs and Class Members provided to it.

170. As alleged herein and above, Defendant's relationship with Representative Plaintiffs and Class Members was governed by promises and expectations that Representative Plaintiffs and Class Members' PHI/PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

171. Representative Plaintiffs and Class Members provided their respective PHI/PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PHI/PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

172. Representative Plaintiffs and Class Members also provided their PHI/PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their PHI/PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting its networks and data systems.

173. Defendant voluntarily received, in confidence, Representative Plaintiffs' and Class Members' PHI/PII with the understanding that the PHI/PII would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

174. Due to Defendant's failure to prevent, detect and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure Representative Plaintiffs' and Class Members' PHI/PII, Representative Plaintiffs' and Class Members' PHI/PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Representative Plaintiffs' and Class Members' confidence and without their express permission.

175. As a direct and proximate cause of Defendant's actions and/or omissions, Representative Plaintiffs and Class Members have suffered damages, as alleged herein.

176. But for Defendant's failure to maintain and protect Representative Plaintiffs' and Class Members' PHI/PII in violation of the parties' understanding of confidence, their PHI/PII

would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. The Data Breach was the direct and legal cause of the misuse of Representative Plaintiffs' and Class Members' PHI/PII and the resulting damages.

177. The injury and harm Representative Plaintiffs and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Representative Plaintiffs' and Class Members' PHI/PII. Defendant knew its data systems and protocols for accepting and securing Representative Plaintiffs' and Class Members' PHI/PII had security and other vulnerabilities that placed Representative Plaintiffs' and Class Members' PHI/PII in jeopardy.

178. As a direct and proximate result of Defendant's breaches of confidence, Representative Plaintiffs and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PHI/PII, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PHI/PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (v) the continued risk to their PHI/PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' PHI/PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members, (vii) the diminished value

of Representative Plaintiffs' and Class Members' PHI/PII, and (viii) the diminished value of Defendant's services for which Representative Plaintiffs and Class Members paid and received.

COUNT FOUR
Breach of Implied Contract
(On behalf of the Nationwide Class)

179. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

180. Through their course of conduct, Defendant, Representative Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiffs' and Class Members' PHI/PII.

181. Defendant required Representative Plaintiffs and Class Members to provide and entrust their PHI/PII as a condition of obtaining Defendant's services.

182. Defendant solicited and invited Representative Plaintiffs and Class Members to provide their PHI/PII as part of Defendant's regular business practices. Representative Plaintiffs and Class Members accepted Defendant's offers and provided their PHI/PII to Defendant.

183. As a condition of being Defendant's direct patients, Representative Plaintiffs and Class Members provided and entrusted their PHI/PII to Defendant. In so doing, Representative Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiffs and Class Members if their data had been breached and compromised or stolen.

184. A meeting of the minds occurred when Representative Plaintiffs and Class Members agreed to, and did, provide their PHI/PII to Defendant, in exchange for, amongst other things, the protection of their PHI/PII.

185. Representative Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

186. Defendant breached the implied contracts it made with Representative Plaintiffs and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised because of the Data Breach.

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

COUNT FIVE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class,
or alternatively, the California, Virginia, and Kansas Subclasses)

187. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

188. Every contract in this State (Connecticut) and the States of the Subclasses (California, Virginia, and Kansas) have an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

189. Representative Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

190. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII, failing to timely and accurately disclose the Data Breach to Representative Plaintiffs and Class Members, and continued acceptance of PHI/PII and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

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

COUNT SIX
Breach of Fiduciary Duty
(On behalf of the Nationwide Class)

192. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

193. In light of the special relationship between Defendant and Representative Plaintiffs and Class Members, whereby Defendant became the guardian of Representative Plaintiffs' and Class Members' PHI/PII, Defendant became a fiduciary by its undertaking and guardianship of the PHI/PII to act primarily for Representative Plaintiffs and Class Members, (i) for the safeguarding of Representative Plaintiffs' and Class Members' PHI/PII, (ii) to timely notify Representative Plaintiffs and Class Members of a data breach and disclosure, and (iii) to maintain complete and accurate records of what information (and where) Defendant did has and continues to store.

194. Defendant has a fiduciary duty to act for the benefit of Representative Plaintiffs and Class Members upon matters within the scope of its relationship with its customers' patients and former patients—in particular, to keep their PHI/PII secure.

195. Defendant breached its fiduciary duties to Representative Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

196. Defendant breached its fiduciary duties to Representative Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Representative Plaintiffs' and Class Members' PHI/PII.

197. Defendant breached its fiduciary duties to Representative Plaintiffs and Class Members by failing to timely notify and/or warn Representative Plaintiffs and Class Members of the Data Breach.

198. Defendant breached its fiduciary duties to Representative Plaintiffs and Class Members by otherwise failing to safeguard Representative Plaintiffs' and Class Members' PHI/PII.

199. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Representative Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PHI/PII, (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PHI/PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, contest, and recover from identity theft, (v) the continued risk to their PHI/PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI/PII in its continued possession, (vi) future costs in terms of time, effort, and money that

will be expended as result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members, and (vii) the diminished value of Defendant's services they received.

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

COUNT SEVEN
Unjust Enrichment
(On behalf of the Nationwide Class)

201. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein. This Count is pled in the alternative to the Breach of Contract Count above.

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

203. As such, a portion of the payments made by or on behalf of Representative Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of each payment allocated to data security is known to Defendant.

204. Representative Plaintiffs and Class Members conferred a monetary benefit to Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and provided Defendant with their PHI/PII. In exchange, Representative Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PHI/PII protected with adequate data security.

205. Defendant knew that Representative Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PHI/PII of Representative Plaintiffs and Class Members for business purposes.

206. Defendant enriched itself by saving the costs it reasonably should have expended in data-security measures to secure Representative Plaintiffs' and Class Members' PHI/PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Representative Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. On the other hand, Representative Plaintiffs and Class Members suffered as a direct and proximate result of Defendant's decision to prioritize its profits over the requisite security.

207. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Representative Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

208. Defendant failed to secure Representative Plaintiffs' and Class Members' PHI/PII and, therefore, did not provide full compensation for the benefit of Representative Plaintiffs and Class Members.

209. Defendant acquired the PHI/PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

210. If Representative Plaintiffs and Class Members knew that Defendant had not reasonably secured their PHI/PII, they would not have agreed to provide their PHI/PII to Defendant.

211. Representative Plaintiffs and Class Members have no remedy at law.

212. As a direct and proximate result of Defendant's conduct, Representative Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of opportunity to determine how their PHI/PII is used, (iii) the compromise, publication, and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (vi) the continued risk to their PHI/PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PHI/PII in its continued possession, and (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

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

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

COUNT EIGHT
Kansas Consumer Protection Act
Kan. Stat. Ann. §§ 50-623 *et seq.*
(On behalf of the Kansas Subclass)

215. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

216. The Kansas Plaintiff, individually (hereinafter "Plaintiff" for purposes of this claim only) and on behalf of the Kansas Subclass, brings this claim.

217. K.S.A. §§ 50-623, *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

218. Plaintiff and Kansas Subclass Members are "consumers" as defined by K.S.A. § 50-624(b).

219. The acts and practices described herein are "consumer transactions," defined by K.S.A. § 50-624(c).

220. Defendant is a "supplier" as defined by K.S.A. § 50-624(l).

221. Defendant advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

222. Defendant engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Kansas Subclass Members' PHI/PII, which was a direct and proximate cause of the Defendant's Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Defendant's Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681(e), the GLBA, 15 U.S.C. § 6801, *et seq.*, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Defendant's Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Kansas Subclass Members' PHI/PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681(e), the GLBA, 15 U.S.C. § 6801, *et seq.*, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Kansas Subclass Members' PHI/PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681(e), the GLBA, 15 U.S.C. § 6801, *et seq.,* and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b.

223. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PHI/PII.

224. Defendant intended to mislead Plaintiff and Kansas Subclass Members and induce them to rely on its misrepresentations and omissions.

225. Had Defendant disclosed to Plaintiff and Kansas Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as a dependable nationwide developer and manager of health services, and Defendant was trusted with sensitive PHI/PII regarding thousands of consumers, including Plaintiff and Kansas Subclass Members. Defendant accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security

controls secret from the public. Accordingly, because Defendant held itself out as having a special role in the healthcare industry with a corresponding duty of trustworthiness and care, Plaintiff and Kansas Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

226. Defendant also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and Kansas Subclass Members to protect their interests reasonably, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and Kansas Subclass Members to enter into a consumer transaction on terms that Defendant knew were substantially one-sided in favor of Defendant (see K.S.A. § 50- 627(b)(5)).

227. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their PHI/PII in Defendant's possession.

228. The above unfair, deceptive and unconscionable practices and acts by Defendant were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass Members that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or competition.

229. Defendant acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act and recklessly disregarded Plaintiff and Kansas Subclass Members' rights.

230. As a direct and proximate result of Defendant's unfair, deceptive and unconscionable trade practices, Plaintiff and Kansas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and nonmonetary damages, including from fraud and identity theft, time, and expenses related to monitoring their

financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their PHI/PII.

231. Plaintiff and Kansas Subclass Members seek all monetary and nonmonetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636, injunctive relief and reasonable attorneys' fees and costs.

COUNT NINE
Virginia Personal Information Breach Notification Act
(Va. Code. Ann. §§ 18.2-186.6, *et seq.*)
(On Behalf of Plaintiff Guerrero and the Virginia Subclass)

232. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

233. The Virginia Plaintiff Guerrero, individually (hereinafter "Plaintiff" for purposes of this claim only) and on behalf of the Virginia Subclass, brings this claim.

234. Defendant is required to accurately notify Plaintiff and Virginia Subclass members following discovery or notification of a breach of their data security system if unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identity theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

235. Defendant is an entity that owns, licenses, or maintains computerized data that includes Personal Information as defined by Va. Code Ann. §§ 18.2-186.6(B), (D).

236. Plaintiff's and Virginia Subclass members' PHI/PII includes Personal Information as covered under Va. Code. Ann. § 18.2-186.6(A).

237. Because Defendant discovered a breach of its security system in which unencrypted or unredacted PHI/PII was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identity theft or

another fraud, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. §§ 18.2-186.6(B), (D).

238. By failing to disclose the Data Breach promptly and accurately, Defendant violated Va. Code Ann. §§ 18.2-186.6 (B), (D).

239. As a direct and proximate result of Defendant's violations of Va. Code Ann. §§ 18.2-186.6(B), (D), Plaintiff and Virginia Subclass members suffered damages, as described above.

240. Plaintiff and Virginia Subclass members seek relief under Va. Coda Ann. § 18.2-186.6(I), including actual damages.

COUNT TEN
Violation of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798, *et seq.*
(On Behalf of Plaintiff Castillo and the California Subclass)

241. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

242. The California Plaintiff Castillo, individually (hereinafter "Plaintiff" for purposes of this claim only) and on behalf of the California Subclass, brings this claim.

243. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual

damages, whichever is greater.
(B) Injunctive or declaratory relief.
(C) Any other relief the court deems proper.

244. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue over $25 million.

245. Plaintiff and California Subclass members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

246. The PHI/PII of Plaintiff and the California subclass at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number, (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual, (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, (iv) medical information, (v) health insurance information, and/or (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

247. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass's PHI/PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PHI/PII of

Plaintiff and the California Subclass. Specifically, Defendant subjected Plaintiff's and the California Subclass's nonencrypted and nonredacted PHI/PII to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

248. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and California Subclass members' PHI/PII included exfiltration, theft, or disclosure through Defendant' servers, systems, and website, and/or the dark web, where hackers further disclosed the PHI/PII alleged herein.

249. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass were injured and lost money or property, including but not limited to the loss of Plaintiff's and the California Subclass's legally protected interest in the confidentiality and privacy of their PHI/PII, stress, fear, and anxiety, nominal damages, and additional losses described above.

250. Section 1798.150(b) specifically provides that "[n]o [prefiling]notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." Accordingly, Plaintiff and the California Subclass by way of this Complaint seek actual pecuniary damages suffered as a result of Defendant's violations described herein.

251. Plaintiff has issued a notice of these alleged violations to Defendant on or about July 11, 2023, pursuant to § 1798.150(b) and intends to amend this Complaint to seek statutory damages and injunctive relief upon expiration of the 30-day cure period pursuant to § 1798(a)(1)(A)-(B), (a)(2), and (b).

COUNT ELEVEN
California Customer Records Act
(On Behalf of Plaintiff Castillo and the California Subclass)

252. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

253. The California Plaintiff Castillo, individually (hereinafter "Plaintiff" for purposes of this claim only) and on behalf of the California Subclass, brings this claim.

254. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

255. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

256. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

257. Plaintiff and members of the California Subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant, directly and/or indirectly, for the purpose of obtaining a service from Defendant.

258. The PHI/PII of Plaintiff and the California Subclass at issue in this lawsuit constitutes "personal information" under §1798.81.5(d)(1) in that the PHI/PII Defendant collects

and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number, (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual, (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, (iv) medical information, (v) health insurance information, and/or (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

259. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass's PHI/PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PHI/PII of Plaintiff and the California Subclass from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the California Subclass's nonencrypted and nonredacted PHI/PII to unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

260. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Representative Plaintiff and the California subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the PHI/PII of Representative Plaintiff and the California Subclass by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

261. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the California Subclass were injured and lost money or property including, but not limited to, the loss of Representative Plaintiff's and the subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

262. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

263. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to

have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

   i. the date of the breach,

   ii. the estimated date of the breach, or

   iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

264. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California Subclass.

265. On information and belief, many California Subclass members affected by the breach, have not received any notice at all from Defendant in violation of Section 1798.82(d).

266. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and California Subclass members suffered incrementally increased damages separate and distinct from those caused by the breaches themselves.

267. As a direct consequence of the actions identified above, Plaintiff and California Subclass members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

COUNT TWELVE
California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiff Castillo and the California Subclass)

268. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

269. The California Plaintiff Castillo, individually (hereinafter "Plaintiff" for purposes of this claim only) and on behalf of the California Subclass, brings this claim.

270. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

271. Defendant violated Cal. Bus. & Prof. Code § 17200 et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

272. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass members' PHI/PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Defendant data breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that trusted entities use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 et seq.), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

273. Defendant engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C.§ 45, and California common law.

274. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass members' PHI/PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass members' PHI/PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties

pertaining to the security and privacy of Plaintiff's and California Subclass members' PHI/PII, including duties imposed by the FTC Act, 15U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass members' PHI/PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150.

275. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

276. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

277. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

278. Plaintiff and California Subclass members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

279. By deceptively storing, collecting, and disclosing their PHI/PII, Defendant has taken money or property from Plaintiff and California Subclass members.

280. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

281. Plaintiff and California Subclass members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT THIRTEEN
California Invasion of Privacy
Cal. Const. Art. 1, § 1
(On Behalf of Plaintiff Castillo and the California Subclass)

282. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

283. The California Plaintiff Castillo, individually (hereinafter "Plaintiff" for purposes of this claim only) and on behalf of the California Subclass, brings this claim.

284. Art. I, § 1 of the California Constitution provides: "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and

liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

285. The right to privacy in California's Constitution creates a private right of action against private and government entities.

286. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (i) a legally protected privacy interest, (ii) a reasonable expectation of privacy, and (iii) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

287. Defendant violated Plaintiff's and California Subclass members' constitutional right to privacy by collecting, storing, and disclosing their PHI/PII in which they had a legally protected privacy interest, and for which they had a reasonable expectation of privacy, in a manner that was highly offensive to Plaintiff and California Subclass members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

288. Defendant has intruded upon Plaintiff's and California Subclass members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential PHI/PII.

289. Plaintiff and California Subclass members had a reasonable expectation of privacy in that: (i) Defendant's invasion of privacy occurred as a result of Defendant's security practices including the collecting, storage, and unauthorized disclosure of consumers' personal information; (ii) Plaintiff and California Subclass members did not consent or otherwise authorize Defendant to disclosure their PHI/PII, and (iii) Plaintiff and California Subclass members could not reasonably expect Defendant would commit acts in violation of laws protecting privacy.

290. As a result of Defendant's actions, Plaintiff and California Subclass members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation.

291. Plaintiff and California Subclass members suffered actual and concrete injury because of Defendant's violations of their privacy interests. Plaintiff and California Subclass members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

292. Plaintiff and California Subclass members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and California Subclass members for the harm to their privacy interests as well as disgorgement of profits made by Defendant because of its intrusions upon Plaintiff's and California Subclass members' privacy.

COUNT FOURTEEN
Declaratory Judgment
(On behalf of the Nationwide Class)

293. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth therein.

294. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

295. An actual controversy has arisen after the Data Breach regarding Representative Plaintiffs' and Class Members' PHI/PII and whether Defendant is currently maintaining data

security measures adequate to protect Representative Plaintiffs and Class Members from further data breaches that compromise their PHI/PII. Representative Plaintiffs allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Representative Plaintiffs continue to suffer injury due to the compromise of their PHI/PII and remain at imminent risk that further compromises of their PHI/PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

296. Representative Plaintiffs and the Classes have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including: (i) Defendant's failure to encrypt Representative Plaintiffs' and Class Members' PHI/PII, including Social Security numbers, while storing it in an Internet-accessible environment, and (ii) Defendant's failure to delete PHI/PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Representative Plaintiffs.

297. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PHI/PII of Representative Plaintiffs and Class Members;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PHI/PII;

c. Defendant's ongoing breaches of its legal duty continue to cause Representative Plaintiffs harm.

298. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law, industry, and government regulatory standards to protect consumers' PHI/PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third-party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards; and

d. implement an education and training program for appropriate employees regarding cybersecurity.

299. If an injunction is not issued, Representative Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Representative Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

300. The hardship to Representative Plaintiffs, if an injunction is not issued, exceeds the hardship to Defendant if an injunction is issued. Representative Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to use such measures.

301. Issuance of the requested injunction will satisfy the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Representative Plaintiffs and others whose confidential information would be further compromised.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on behalf of themselves and each member of the proposed National Class, the California Subclass, the Virginia Subclass, and the Kansas Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from similar unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiffs' and Class Members' PHI/PII, and from refusing to issue prompt, complete, and accurate disclosures to Representative Plaintiffs and Class Members;

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

   a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

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

c. requiring Defendant to delete and purge Representative Plaintiffs' and Class Members' PHI/PII unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' PHI/PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' PHI/PII on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Representative Plaintiffs and Class Members;

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

k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested and updated;

l. requiring Defendant to meaningfully educate all Class Members about the threats they face as a result of the loss of their confidential PHI/PII to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law;

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demand a trial by jury for all issues triable by jury.

Dated: July 26, 2023

LAUKAITIS LAW LLC

By: */s/ Kevin Laukaitis*

Kevin Laukaitis, Esq. (admitted *pro hac vice*)
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
Telephone: (215) 789-4462
Email: klaukaitis@laukaitislaw.com

Laura Van Note, Esq. (admitted *pro hac vice*)
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: lvn@colevannote.com

Co-Lead Counsel for Representative Plaintiffs and the Proposed Class(es)

Erin Green Comite, Esq. (ct24886)
Anja Rusi, Esq. (ct30686)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
156 S. Main St.
P.O. Box 192
Colchester, CT 06415
Telephone: (860) 537-5537
Facsimile: (860) 537-4432
Email: ecomite@scott-scott.com

Joseph P. Guglielmo, Esq. (ct27481)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334

Liaison Counsel for Representative Plaintiffs and the Proposed Class(es)