Exhibit A

Scott Edward Cole, Esq. (CA S.B. #160744)*
Laura Grace Van Note, Esq. (CA S.B. #310160)*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Tel: (510) 891-9800
Email: sec@colevannote.com
Email: lvn@colevannote.com

Bryan L. Bleichner (CA S.B. # 220340)*
Philip J. Krzeski (MN S.B. #0403291)*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Tel: (612) 339-7300
Email: bbleichner@chestnutcambronne.com
Email: pkrzeski@chestnutcambronne.com

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

**Admitted pro hac vice*

Interim Co-Lead Class Counsel

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

THOMAS BYERS, SKYLER GRENN, and KAREN PRESTEGARD, individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

ORTHOALASKA, LLC,

Defendant.

Case No. 3:23-cv-00242-SLG
(Consolidated Lead Case)

CONSOLIDATED CLASS ACTION COMPLAINT

[Jury Trial Demanded]

1. Representative Plaintiffs Thomas Byers, Skyler Grenn and Karen Prestegard ("Representative Plaintiffs") bring this class action against Defendant OrthoAlaska, LLC ("Defendant" or "OrthoAlaska") 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 and addresses, dates of birth, Social Security numbers, payment card numbers, driver's license and/or state identification numbers, account and routing numbers, health insurance and medical information[1] (these types of information, *inter alia*, being thereafter referred to as "protected health information" or "PHI"[2] and "personally identifiable information" or "PII," collectively referred to as "PHI/PII").[3]

2. With this action, Representative Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiffs and,

---

[1] A sample copy of the Notice letter is available at https://apps.web.maine.gov/online/aeviewer/ME/40/29e7dc48-81ff-4eb9-802d-2b59d6b1274c.shtml (last accessed December 8, 2023).

[2] 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.

[3] 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.).

at least, 161,130 other similarly situated persons[4] in the massive and preventable cyberattack purportedly, discovered by Defendant on October 12, 2022, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PHI/PII which was being kept unprotected (the "Data Breach").

3. Representative Plaintiffs further seek to hold Defendant responsible for not ensuring that the 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 October 12, 2022, Defendant did not begin informing victims of the Data Breach until October 11, 2023 and failed to inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiffs and Class Members were wholly unaware of the Data Breach until they received letters from Defendant informing them of it (the "Notice"). The Notices received by Representative Plaintiffs were dated October 11, 2023.

5. Defendant is a healthcare limited liability company and "an integrated group of orthopedic, rheumatology and primary care providers in Alaska[.]"[5]

---

[4] "Data Breach Notifications," Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/69f35b42-efc4-43a8-b450-9046f5ce2243.shtml/ (last accessed December 8, 2023).

[5] https://www.orthoak.net/ (last accessed December 8, 2023).

6. 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.

7. HIPAA establishes national minimum standards for the protection of individuals' medical records and other protected health information. HIPAA generally applies to health plans and 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.

8. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information that is 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.

9. 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 and other state and federal statutes and regulations as well as 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.

10. 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 an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, 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 their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

11. 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 other Class Member is a citizen of a state different from Defendant.

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

13. Defendant is headquartered and routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

14. 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 does business in this Judicial District.

PLAINTIFFS

Thomas Byers

15. Representative Plaintiff Thomas Byers is an adult individual and, at all relevant times herein, was a resident and citizen of the State of Alaska. Representative Plaintiff is a victim of the Data Breach.

16. Plaintiff Byers did not receive Notice of the Data Breach from the Defendant until on or about October 11, 2023. The Defendant's Notice stated that his date of birth, medical information, and health insurance information was involved.

17. Following the breach, Plaintiff Byers' has been receiving suspicious bank statements, magazines delivered to Byers' home with another person's name on them as the recipient but using Plaintiff Byers' address, a high increase in SPAM calls, etc.

18. The Data Breach has caused Plaintiff Byers to suffer significant fear, anxiety, and stress.

Karen Prestegard

19. Representative Plaintiff Karen Prestegard is an adult individual and, at all relevant times herein, was a resident and citizen of Anchorage Municipality of Anchorage, Alaska.

20. Plaintiff Prestegard received medical services through Defendant. As a condition to receiving the medical services, Plaintiff Prestegard provided her Private Information to Defendant, with the expectation that the Private Information would be

safeguarded against cyberattacks and foreseeable theft and would not disclosed for unauthorized purposes.

21. Although Defendant learned that the Data Breach occurred on or about October 12, 2022, Plaintiff Prestegard did not receive Notice of the Data Breach from the Defendant until on or about October 11, 2023. The Defendant's Notice stated that her date of birth, medical information, and health insurance information was involved.

22. The Data Breach has caused Plaintiff Prestegard to suffer significant fear, anxiety, and stress. Plaintiff Prestegard has lost sleep thinking about all the ways the Private Information that was exposed can be used to commit fraud and identity theft.

23. Upon receiving the Notice, Plaintiff Prestegard requested three copies of her credit reports the same week that she received the Notice.

Skyler Grenn

24. Representative Plaintiff Skyler Grenn is an adult individual and, at all relevant times herein, was a resident and citizen of Anchorage, Alaska.

25. Each of the Representative Plaintiffs received notices from Defendant regarding the cybersecurity event, read the notices, and then took action to research and otherwise address the potential adverse consequences of their PHI/PII having been exposed through the event. Had Defendant taken proper care of Representative Plaintiffs private information and had not otherwise committed the violations detailed herein, Representative Plaintiffs would not have taken such actions and would not otherwise be damaged as detailed in this pleading.

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

27. At all times herein relevant, Representative Plaintiffs are and were members of the Class.

28. As required in order to obtain services from Defendant, Representative Plaintiffs provided Defendant with highly sensitive PHI/PII. Other than this, Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

29. Plaintiffs are very careful about sharing their sensitive Private Information. Plaintiffs store any documents containing their Private Information in a safe and secure location. They have never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiffs would not have entrusted their Private Information to Defendant had he known of Defendant's lax data security policies.

30. Representative Plaintiffs' PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Representative Plaintiffs' PHI/PII. Representative Plaintiffs' PHI/PII was within the possession and control of Defendant at the time of the Data Breach.

31. Representative Plaintiffs received a letter from Defendant, dated October 11, 2023, stating Representative Plaintiffs' PHI/PII was involved in the Data Breach.

32. As a result, Representative Plaintiffs spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring their accounts and seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

33. 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 as a result of the Data Breach.

34. Representative Plaintiffs suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has 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.

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

36. Representative Plaintiffs has 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.

DEFENDANT

37. Defendant is an Alaska limited liability corporation with a principal place of business located at 3801 Lake Otis Parkway, Suite 300, Anchorage, Alaska 99508. Defendant is comprised of a group of orthopedic, rheumatology and primacy care providers in Alaska and is the entity that owned, operated, and maintained the health system that was compromised in the Data Breach. Defendant touts that it "was created to address the rising costs of health care in Alaska"[6] and make clear through advertising and web presence that it is primarily engaged in the health care industry. As such, Defendant routinely acquired, utilized, and stored Plaintiffs' and Class Member's PHI and PII, and accepted heightened duties of care over said information as a result of its special relationship with Class Members. Upon information and belief, Defendant employs more than 250 employees and has at least three locations across Alaska.

38. 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

[6] "About," OrthoAlaska, https://www.orthoak.net/about/ (last accessed December 8, 2023).

leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

39. Representative Plaintiffs brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiffs and the following class(es)/subclass(es) (collectively, the "Class"):

> **Nationwide Class:**
> "All individuals within the United States of America whose PHI/PII was impacted as a result of the Data Breach allegedly discovered by Defendant on October 12, 2022."

40. Excluded from the Class 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.

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

42. Representative Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

43. This action has been brought and may properly be maintained as a class action under Federal Rules of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed Class is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiffs Class 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 tens of thousands of individuals. Membership in the Class 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 Class 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 Representative Plaintiffs' and Class Members' PHI/PII;

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; and

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 Plaintiffs Class. Representative Plaintiffs and all members of the Plaintiffs Class 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 the Plaintiffs Class in that the Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to 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 Class in its entirety.

Representative Plaintiffs anticipates no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. 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 the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

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

45. 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 with respect to the Class in its entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Representative Plaintiffs.

46. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PHI/PII of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

47. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

48. In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' sensitive data, including but not limited to, their full names, dates of birth, Social Security numbers, health insurance information and medical information. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

49. According to the Data Breach Notification, which Defendant filed with the Office of the Maine Attorney General, 161,130 persons were affected by the Data Breach.[7] Representative Plaintiffs were provided the information detailed above upon

[7] "Data Breach Notifications," Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/69f35b42-efc4-43a8-b450-9046f5ce2243.shtml/ (last accessed December 8, 2023).

Representative Plaintiffs' receipts of letters from Defendant, dated October 11, 2023. Representative Plaintiffs were not aware of the Data Breach until receiving that letter.

Defendant's Failed Response to the Breach

50. 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. According to Defendant, it learned of the Data Breach on October 12, 2022.

51. Not until roughly a *year* after it claims to have discovered the Data Breach, however, did Defendant begin sending the Notice to persons whose PHI/PII Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendant's recommended next steps. Specifically, the Notice informed Plaintiffs and Class Members, in relevant part, that:

> **What happened?** On October 12, 2022, OrthoAlaska discovered unauthorized activity on our systems. In response, we immediately began containment, mitigation, and restoration efforts to terminate the activity and to secure our network, systems, and data. In addition, we retained independent cybersecurity experts to conduct a forensic investigation into the incident and assist us in determining what happened. This forensic investigation determined that there was unauthorized access to files stored within our systems that contain information about our patients.

52. In the Notice Letter, Defendant offers to provide credit monitoring and identity theft insurance services for a period of no longer than 24 months. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years

of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services. Defendant's offer of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive Private Information was in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

Defendant Collected But Then Negligently Stored Class Members' PHI/PII

53. Defendant acquired, collected, stored and assured reasonable security over Representative Plaintiffs' and Class Members' PHI/PII as a condition of its relationships with Representative Plaintiffs and Class Members. Indeed, 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.

54. 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.

55. By obtaining, collecting, and storing Representative Plaintiffs' and Class Members' PHI/PII, 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.

56. 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 purposes only and to make only authorized disclosures of this information.

57. Defendant could have prevented the Data Breach, which began no later than October 12, 2022, by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiffs' and Class Members' PHI/PII, but failed to do so.

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

59. 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 its industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

60. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' PHI/PII from being compromised in a variety of ways including:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

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

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

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

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption"); and

o. Failing to adhere to industry standards for cybersecurity.

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

Defendant Had a HIPPA Obligation to Protect the Stolen Information

62. 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 have an affirmative duty to keep patients' PHI/PII confidential. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiffs' and Class Members' PHI/PII. Moreover, Representative Plaintiffs and Class Members surrendered their highly sensitive PHI/PII to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their PHI/PII, independent of any statute.

63. Because Defendant is a covered entity under 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.

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

65. 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.

66. 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.

67. "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.

68. 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.

69. 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).

70. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[8] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

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

74. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. See 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in

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

identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[9] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[10]

75. 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."

Defendant Had An Obligation under the FTC Act to Protect the Stolen Information

76. 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'

[9] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.(last accessed December 8, 2023).

[10] http://www.hhs.gov/hipaa/for-professionals/security/guidance/ index.html.https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html/ (last accessed December 8, 2023).

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).

77. In October 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

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

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data

as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. These FTC enforcement actions include actions against healthcare entities, like Defendant. *See, e.g., In the Matter of LabMd, Inc*., A Corp, 2016-2 Trade Cas. (Henry Ford) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

81. Indeed, as detailed above, data breaches are preventable.[11] 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."[12] 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…."[13]

82. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[14]

---

[11] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[12] Id. at 17.
[13] Id. at 28.
[14] Id.

Defendant Had an Implied Contractual Obligation to Protect the Stolen Information

83. In addition to its obligations under federal and state laws, Defendant promised Representative Plaintiffs and Class Members that it would keep their information secure. Indeed, Defendant directs patients to the Privacy Policy on Orthopedic Physicians Alaska's website, which provides that: "[o]ur Practice is dedicated to maintaining the privacy of your Individually Identifiable Health Information (IIHI). . . We are required by law to maintain the confidentiality of health information that identifies you."[15]

84. Thus, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for the provision of healthcare services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Defendant Had a Duty of Reasonable Care to Protect the Stolen Information

85. In addition to its obligations under federal and state laws and/or implied contracts, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and

[15] https://opalaska.com/wp-content/uploads/2022/10/opa_privacy.pdf (last accessed (last accessed December 8, 2023).

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.

86. 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.

87. 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 maintained substandard data security systems.

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

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

90. 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 their PHI/PII to Defendant.

91. 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.

92. 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 in order to identity possible threats.

Value of the Sensitive Information

93. 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."

94. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[16] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[17] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which

[16] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed December 8, 2023).

[17] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed December 8, 2023).

account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[18]

95. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[19] According to cybersecurity firm Mimecast, 90 percent of healthcare organizations experienced cyber-attacks in 2019 alone.[20]

96. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

97. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so

---

[18] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/ (last accessed December 8, 2023).

[19] https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed December 8, 2023).

[20] See Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attach (last accessed December 8, 2023).

they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[21]

98. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain PHI/PII compromised in the 2017 Equifax data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the State of Oklahoma. Indeed, as companies became more dependent on computer systems to run their business,[22] *e.g.*, working remotely as a result of the COVID-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[23]

99. 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 plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, medical prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the

---

[21] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware (last accessed December 8, 2023).

[22] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html/ (last accessed December 8, 2023).

[23] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and- banking-firms-in-2022. (last accessed December 8, 2023).

dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites.

100. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[24]

101. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[25]

---

[24] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed December 8, 2023).

[25] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed December 8,

102. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

103. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

104. Data breaches at healthcare providers like Defendant are especially problematic because the breaches can negatively impact the overall daily lives of individuals affected by the attack.

105. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment because of the disruption of service. This leads to a deterioration in the quality of overall care patients receive at facilities affected by data breaches.

106. Researchers have found that, among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[26] Researchers have further found that at medical service

2023).

[26] *See*, Nsikan Akpan, Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-

providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[27]

107. Similarly, data breach incidents cause patients issues with receiving care that rise above the level of mere inconvenience. The issues that patients encounter as a result of such incidents include, but are not limited to:

a. rescheduling their medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. inability to access their medical records.[28]

108. The high value of PHI/PII to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from

---

other-databreaches- linked-to-uptick-in-fatal-heart- attacks (last accessed December 8, 2023).

[27] *See*, Sung J. Choi et al., Cyberattack Remediation Efforts and Their Implications for Hospital Quality, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last accessed December 8, 2023).

[28] See, e.g., Lisa Vaas, Cyberattacks Paralyze, and Sometimes Crush, Hospitals, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze- andsometimes-crush-hospitals// (last accessed December 8, 2023); Jessica David, Data Breaches Will Cost Healthcare $4B in 2019. Threats Outpace Tech, Health IT Security (Nov. 5, 2019), https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats- outpacetech - :~:text=No

$40 to $200, and bank details have a price range of $50 to $200.[29] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[30] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[31] According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.[21] As Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[32]

109. Identity thieves can use PHI/PII, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of 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.

---

[29] 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 December 8, 2023).

[30] 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 December 8, 2023).

[31] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed December 8, 2023).

[32] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x- price-of-stolen-credit-card-numbers.html (last accessed December 8, 2023).

110. 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.[33]

111. The ramifications of Defendant's failure to keep 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, Representative Plaintiffs' and Class Members' PHI/PII 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.

112. 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

[33] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf/ (last accessed December 8, 2023).

in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[34]

113. "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."[35]

114. 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.

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

---

[34] 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 December 8, 2023).

[35] Id.

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

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

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

119. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[36]

[36] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a

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

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

---

victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. See, e.g., Brian Krebs, Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-] (https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in- underground-stolen-from-texas-life-insurance-finn/ (last accessed December 8, 2023).

122. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the Data Breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other Class Members.

123. Thus, even if certain information (such as Social Security numbers) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

124. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

125. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[37] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[38]

126. 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

[37] 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 December 8, 2023).

[38] 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 December 8, 2023).

Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant knew or should have known that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Its failure to do so is therefore intentional, willful, reckless and/or grossly negligent.

Present and Future Harm to Plaintiffs

127. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach, changing passwords and resecuring their own computer networks, and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

128. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[39]

129. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information

[39] *See*, United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007); https://www.gao.gov/new.items/d07737.pdf.

after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[40]

130. Today, Representative Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used and what steps are being taken, if any, to secure their PHI/PII going forward. Representative Plaintiffs and Class Members are thus 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 exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

131. Representative Plaintiffs' and Class Members' PHI/PII may end up for sale on the dark web, or simply 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.

Diminution Value Of Private Information

[40] *See,* Federal Trade Commission, Identity Theft.gov; https://www.identitytheft.gov/Steps (last accessed December 8, 2023).

132. PII and PHI are valuable property rights.[41] Their value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

133. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[42]

134. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[43]

135. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[44]

136. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[45]

---

41 *See,* e.g., Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

42 https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed December 8, 2023).

43 https://datacoup.com/; https://digi.me/what-is-digime/ (last accessed December 8, 2023).

44 Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

45 See Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed December 8, 2023).

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of the Nationwide Class)

137. 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.

138. 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.

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

140. Defendant knew that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject

Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

141. 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 about numerous, well-publicized data breaches.

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

143. 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.

144. 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 Representative Plaintiffs' and Class Members' PHI/PII.

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

146. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with its PHI/PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to 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.

147. 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 and Representative Plaintiffs and/or the remaining Class Members.

148. 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 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 the 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 to not store PHI/PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiffs' and the 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.

149. 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.

150. 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 harms and damages (as alleged above).

151. 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.

152. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting roughly a year 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.

153. Furthermore, through its failure 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, *inter alia*, secure and/or access their PHI/PII.

154. 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 suffered, 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.

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

156. 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.

157. 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.

158. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PHI/PII and 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 Plaintiffs and Class Members.

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

160. 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 personal records, (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.

161. 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 noneconomic losses.

162. 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.

SECOND CLAIM FOR RELIEF
Invasion of Privacy
(On behalf of the Nationwide Class)

163. 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.

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

165. Defendant owed a duty to its current and former patients, including Plaintiffs and the Nationwide Class, to keep their Private Information contained as a part thereof, confidential.

166. Defendant failed to protect and actually or potentially released to unknown and unauthorized third parties the Private Information of Plaintiffs and the Nationwide Class.

167. Defendant allowed unauthorized and unknown third parties to actually or potentially access and examine the Private Information of Plaintiffs and the Nationwide Class, by way of Defendant's failure to protect the Private Information. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and the Nationwide Class is highly offensive to a reasonable person.

168. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Nationwide Class disclosed their Private Information to

Defendant as part of Plaintiffs' and the Class Members' relationships with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure.

169. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

171. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class.

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

173. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class in that the Private Information maintained by Defendant can be viewed, distributed,

and used by unauthorized persons for years to come. Plaintiffs and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Nationwide Class)

174. 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.

175. 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.

176. Defendant required Representative Plaintiffs and Class Members to provide and entrust their PHI/PII as a condition of obtaining Defendant's goods/services/employment from/with Defendant.

177. 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.

178. As a condition of being direct customers and/or employees of Defendant, 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 its data had been breached and compromised or stolen.

179. 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.

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

181. 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 as a result of the Data Breach.

182. As a direct and proximate result of Defendant's above-described breach of implied contract, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for the provision of healthcare services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value

than what they reasonably expected to receive under the bargains they struck with Defendant.

183. As a further 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 noneconomic harm.

FOURTH CLAIM FOR RELIEF
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class)

184. 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.

185. Every contract in this State has 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.

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

187. 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.

188. 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.

FIFTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On behalf of the Nationwide Class)

189. 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.

190. Plaintiffs and Class Members gave Defendant their Private Information in confidence, believing that Defendant would protect that information. Plaintiffs and Class Members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiffs' and Class Members' Private Information created a fiduciary relationship between Defendant and the Plaintiffs and Class Members. In light of this relationship, Defendant must act primarily for the benefit of the Plaintiffs and the Class Members, which includes taking appropriate steps to safeguard and protect their Private Information.

191. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship.

192. Defendant breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' Private Information, failing to comply with the applicable data security laws, standards, and guidelines, and otherwise failing to safeguard Plaintiffs' and Class Members' Private Information that it collected.

193. As a direct and proximate result of the breach of the contractual duties, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include (a) the invasion of privacy, (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' Private Information, (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity, (d) monetary costs associated with the detection and prevention of identity theft, (e) economic costs, including time and money, related to incidents of actual identity theft, (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information, (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendant promised when Plaintiffs and the proposed class entrusted Defendant with their Private Information, and (h) the continued and substantial risk to Plaintiffs and Class Members Private Information, which remains in the Defendant's possession of Defendant with inadequate measures to protect Plaintiffs' and Class Members' Private Information.

SIXTH CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of the Nationwide Class)

194. 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.

195. This Count is brought in the alternative to the breach of implied contract count above.

196. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for healthcare services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the healthcare services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

197. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving healthcare services from Defendant. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

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

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

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

201. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

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

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

204. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense

of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

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

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

207. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on Representative Plaintiffs' own behalf and on behalf of each member of the proposed National Class, respectfully request that the Court enter judgment in favor of Representative Plaintiffs and the Class 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 the proposed Class and/or any other appropriate subclasses under Federal Rules of Civil Procedure Rule 23 (b)(1), (b)(2), and/or (b)(3), including 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 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 security 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 personally identifiable information;

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

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

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

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

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

JURY DEMAND

Representative Plaintiffs, individually and on behalf of the Plaintiffs Class and/or subclasses, hereby demand a trial by jury for all issues triable by jury.

Dated: December 13, 2023

By: */s/ Scott Edward Cole* _____

Scott Edward Cole, Esq. (CA S.B. #160744)*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Tel: (510) 891-9800
Email: sec@colevannote.com

Bryan L. Bleichner (CA S.B. # 220340)*
Philip J. Krzeski (MN BAR #0403291)*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Tel: (612) 339-7300
Email: bbleichner@chestnutcambronne.com
Email: pkrzeski@chestnutcambronne.com

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

*Admitted *pro hac vice*

Attorneys for Representative Plaintiffs and the Plaintiffs Class

CERTIFICATE OF SERVICE

I hereby certify that, on December 13, 2023, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF. I also certify the foregoing document is being served today on all counsel of record in this case via transmission of Notice of Electronic Filing generated by CM/ECF and on counsel in the related cases to their respective emails per the below service list.

/s/ Scott Edward Cole
Scott Edward Cole, Esq.