IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

DEON NELSON and CAROL DEPRIEST individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

RADIOLOGY ASSOCIATES OF ALBUQUERQUE, P.A. and ADVANCED IMAGING, LLC,

Defendants.

Case No.

CLASS ACTION

JURY TRIAL DEMANDED

Representative Plaintiffs alleges as follows:

INTRODUCTION

1. Representative Plaintiffs Deon Nelson and Carol Depriest ("Representative Plaintiffs"), bring this class action against Defendants Radiology Associates of Albuquerque, P.A. and Advanced Imaging ("Defendants") for their failure to properly secure and safeguard Representative Plaintiffs' and Class Members' protected health information and personally identifiable information stored within Defendants' information network, including, without limitation, name, Social Security number, date of birth, patient identification number, billing information, and exam type (these types of information, *inter alia*, being thereafter referred to, collectively, as "protected health information" or "PHI"[1] and "personally identifiable information" or "PHI/PII").[2]

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

[2] Personally identifiable information ("PHI/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

2. With this action, Representative Plaintiffs seek to hold Defendants responsible for the harms they caused and will continue to cause Representative Plaintiffs and, at least, 501[3] others similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendants in August of 2021, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PHI/PII and financial information belonging to both adults and children, which was being kept unprotected (the "Data Breach").

3. Representative Plaintiffs further seek to hold Defendants 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 ("HIPPA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPPA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164), and other relevant standards.

4. While Defendants claims to have discovered the breach as early as August of 2021, Defendants did not begin informing victims of the Data Breach until September 9, 2022 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 Defendants informing them of it. The notice received by Representative Plaintiffs was dated September 9, 2022.

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

6. HIPAA establishes national minimum standards for the protection of individuals' medical records and other personal health information. HIPAA, generally, applies to health plans/insurers, health care clearinghouses, and those health care providers that conduct certain

---

that on its face expressly identifies an individual. PHI/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).

[3] *Breach Portal*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed September 21, 2022).

health care 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 Defendants to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Representative Plaintiffs' and Class Members' PHI/PII, including rights to examine and obtain copies of their health records, and to request corrections thereto.

7. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal 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.

8. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiffs' and Class Members' PHI/PII, Defendants 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 does not bring claims in this action for direct violations of HIPAA, but charges Defendants with various legal violations merely predicated upon the duties set forth in HIPAA.

9. Defendants disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly, 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, the PHI/PII of Representative Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class

Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

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

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

12. Defendants' principal place of business is in New Mexico, and it is domiciled in this judicial district for purposes of jurisdiction.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because the events that gave rise to Representative Plaintiffs' claims took place within the District of New Mexico, and Defendants are headquartered in this Judicial District.

PLAINTIFFS

14. Representative Plaintiffs are adult individuals and, at all relevant times herein, residents and citizens of New Mexico. Representative Plaintiffs are victims of the Data Breach.

15. Defendants received highly sensitive personal, medical, and financial information from Representative Plaintiffs in connection with the imaging services they had received or requested therefrom. As a result, Representative Plaintiffs' information was among the data accessed by an unauthorized third-party in the Data Breach.

16. Representative Plaintiffs received (and were "consumers" for purposes of obtaining) services from Defendants within this state.

17. At all times herein relevant, Representative Plaintiffs are and were members of each of the Classes.

18. As required in order to obtain services from Defendants, Representative Plaintiffs provided Defendants with highly sensitive personal, financial, health and insurance information.

19. Representative Plaintiffs' PHI/PII was exposed in the Data Breach because Defendants stored and/or shared Representative Plaintiffs' PHI/PII and financial information. Their PHI/PII and financial information was within the possession and control of Defendants at the time of the Data Breach.

20. Representative Plaintiffs received a letter from Defendants, dated September 9, 2022, stating that their PHI/PII and/or financial information was involved in the Data Breach (the "Notice").

21. 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.

22. Representative Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PHI/PII—a form of intangible property that they entrusted to Defendants, which was compromised in and as a result of the Data Breach.

23. Representative Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling their PHI/PII and/or financial information.

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

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

DEFENDANT

26. Defendants are New Mexico corporations, each with a principal place of business located at 4411 The 25 Way NE, Suite 150, Albuquerque, NM 87109.

27. Defendants provide imaging services for patients from facilities in New Mexico. Defendants have provided these services for more than 45 years.[4]

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

CLASS ACTION ALLEGATIONS

29. 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 classes/subclass(es) (collectively, the "Classes"):

> **Nationwide Class:**
> "All individuals within the United States of America whose PHI/PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach discovered by Defendants in August 2021."
>
> **New Mexico Subclass:**
> "All individuals within the State of New Mexico whose PHI/PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach discovered by Defendants in August 2021."

30. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards,

[4] https://www.raaonline.com/who-we-are/ (last accessed September 21, 2022)]

sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

31. Also, in the alternative, Representative Plaintiffs request additional Subclasses as necessary based on the types of information that was compromised.

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

33. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed classes 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 Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiffs is informed and believes and, on that basis, alleges that the total number of Class Members is in the hundreds of thousands of individuals. Membership in the Classes will be determined by analysis of Defendants' records.

b. Commonality: Representative Plaintiffs and the Class Members share a community of interests 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 Defendants had a legal duty to Representative Plaintiffs and the Classes to exercise due care in collecting, storing, using, and/or safeguarding their PHI/PII/PHI;

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

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

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

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

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

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

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

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

10) 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 Defendants' wrongful conduct;

11) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

c. Typicality: Representative Plaintiffs' claims are typical of the claims of the Plaintiffs Classes. Representative Plaintiffs and all members of the Plaintiffs Classes sustained damages arising out of and caused by Defendants' common course of conduct in violation of law, as alleged herein. The same event and conduct that gave rise to Representative Plaintiffs' claims are identical to those that give rise to the claims of every Class Member because Representative Plaintiffs and Class Members alike had their Stored Data compromised in the same way by the same conduct of Defendants. Representative Plaintiffs and Class Members face identical threats resulting from the resetting of their hard drives and/or access by cyber-criminals to the Stored Data maintained thereon.

d. Adequacy of Representation: Representative Plaintiffs in this class action is an adequate representative of each of the Plaintiffs Classes in that Representative Plaintiffs has the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case, and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Classes in their entirety. Representative Plaintiffs anticipates no management difficulties in this litigation. Representative Plaintiffs and its counsel will fairly and adequately protect the interests of all Class Members.

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

> case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

34. This class action is also appropriate for certification because Defendants have 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. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendants' conduct with respect to the Class in its entirety, not on facts or law applicable only to Representative Plaintiffs.

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

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

COMMON FACTUAL ALLEGATIONS

The Cyberattack

37. In the course of the Data Breach, one or more unauthorized third-parties accessed Class Members' sensitive data including, but not limited to name, Social Security number, date of birth, patient identification number, billing information, and exam type. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

38. According to the Data Breach Notification, which Defendants filed with the United States Department of Health and Human Services, 501 persons were affected by the Data Breach.[5]

[5] Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed September 21, 2022).

39. Representative Plaintiffs were provided the information detailed above upon their receipt of a letter from Defendants, dated on or about September 9, 2022. Representative Plaintiffs were not aware of the Data Breach.

Defendants' Failed Response to the Breach

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

41. Not until roughly one year after it claims to have discovered the Data Breach did Defendants begin sending the Notice to persons whose PHI/PII and/or financial information Defendants confirmed was potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendants' recommended next steps.

42. The Notice included, *inter alia*, the claims that Defendants had learned of the Data Breach in August of 2021 and had taken steps to respond.

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

44. Defendants have and continue 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.

45. Representative Plaintiffs and Class Members were required to provide their PHI/PII and financial information to Defendants in order to receive healthcare, and as part of providing healthcare, Defendants created, collected, and stored Representative Plaintiffs and Class Members with the reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

46. Despite this, 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 and financial information 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 Defendants intend to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

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

Defendants Collected/Stored Class Members' PHI/PII and Financial Information

48. Defendants acquired, collected, and stored and assured reasonable security over Representative Plaintiffs' and Class Members' PHI/PII and financial information.

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

50. By obtaining, collecting, and storing Representative Plaintiffs' and Class Members' PHI/PII and financial information, Defendants assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Representative Plaintiffs' and Class Members' PHI/PII and financial information from unauthorized disclosure.

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

52. Defendants could have prevented the Data Breach, which began as early as July 22, 2021, by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiffs' and Class Members' PHI/PII and financial information.

53. Defendants' negligence in safeguarding Representative Plaintiffs' and Class Members' PHI/PII and financial information 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.

54. The healthcare industry has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint and cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[6] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported in April 2021.[7]

55. For example, Universal Health Services experienced a cyberattack on September 29, 2020 that appears similar to the attack on Defendants. As a result of this attack, Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[8] Similarly, in 2021, Scripps Health suffered a cyberattack, an event which effectively shut down critical health care services for a month and left numerous

[6] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/ (last accessed November 5, 2021).
[7] https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last accessed November 5, 2021).
[8] https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and (last accessed November 5, 2021).

patients unable to speak to its physicians or access vital medical and prescription records.[9] A few months later, University of San Diego Health suffered a similar attack.[10]

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

57. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' PHI/PII and financial information from being compromised.

Defendants Had an Obligation to Protect the Stolen Information

58. Defendants' failure to adequately secure Representative Plaintiffs' and Class Members' sensitive data breaches duties it owes Representative Plaintiffs and Class Members under statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to keep patients' Protected Health Information private. As a covered entity, Defendants have a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiffs' and Class Members' data. Moreover, Representative Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendants would keep it private and secure. Accordingly, Defendants also have an implied duty to safeguard their data, independent of any statute.

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

[9] https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/ (last accessed November 5, 2021).
[10] https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/ (last accessed November 5, 2021).

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

61. 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.

62. HIPAA requires Defendants 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.

63. "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.

64. HIPAA's Security Rule requires Defendants to do the following:

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

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

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

d. Ensure compliance by its workforce.

65. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" 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).

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

67. Defendants were also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

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

69. Defendants owed a duty to Representative Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PHI/PII and financial information in its possession was adequately secured and protected.

70. Defendants owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PHI/PII and financial information in its possession, including not sharing information with other/her/their entities who maintained sub-standard data security systems.

71. Defendants 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.

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

73. Defendants 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 and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PHI/PII and/or financial information to Defendants.

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

75. Defendants owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' PHI/PII and financial information and monitor user behavior and activity in order to identity possible threats.

Value of the Relevant Sensitive Information

76. 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, RX's, treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII and financial information are valuable commodities 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. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

77. The high value of PHI/PII and financial information to criminals is further evidenced by the prices they will pay 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 $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports

[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[13]

78. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[14] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[15] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03% of overall health data breaches, according to cybersecurity firm Tenable.[16]

79. 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 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

80. 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."

---

[12] *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 November 5, 2021).

[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed January 21, 2022).

[14] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 (last accessed January 21, 2022).

[15] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed January 21, 2022).

[16] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed January 21, 2022).

81. Identity thieves can use PHI/PII and financial information, such as that of Representative Plaintiffs and Class Members which Defendants 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.

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

83. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

84. The harm to Representative Plaintiffs and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed January 21, 2022).

2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[18]

85. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[19]

86. When cyber criminals 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 Defendants may have exposed Representative Plaintiffs and Class Members.

87. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[20] Almost half of medical identity theft victims lose its healthcare coverage as a result of the incident, while nearly one-third saw its insurance premiums rise, and forty percent were never able to resolve its identity theft at all.[21]

88. And data breaches are preventable.[22] 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."[23] She/he/they 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 . . . ."[24]

---

[18] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed January 21, 2022).
[19] *Id.*
[20] 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 January 21, 2022).
[21] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed January 21, 2022).
[22] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[23] *Id.* at 17.
[24] *Id.* at 28.

89. 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*."[25]

90. Here, Defendants knew of the importance of safeguarding PHI/PII and financial information and of the foreseeable consequences that would occur if Representative Plaintiffs' and Class Members' PHI/PII and financial information was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendants are a sophisticated organizations with the resources to deploy robust cybersecurity protocols. They 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.

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

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of the Nationwide Class and the New Mexico Subclass)

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

[25] *Id.*

90. At all times herein relevant, Defendants 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 financial information and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing the PHI/PII and financial information of Representative Plaintiffs and Class Members in its computer systems and on its networks.

91. Among these duties, Defendants were expected:

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

b. to protect Representative Plaintiffs' and Class Members' PHI/PII and financial information 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 and financial information.

92. Defendant knew that the PHI/PII and financial information was private and confidential and should be protected as private and confidential. Therefore, Defendants 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.

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

94. Defendants knew, or should have known, that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' PHI/PII and financial information.

95. Only Defendants were in the position to ensure that its systems and protocols were sufficient to protect the PHI/PII and financial information that Representative Plaintiffs and Class Members had entrusted to it.

96. Defendants breached their duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PHI/PII and financial information of Representative Plaintiffs and Class Members.

97. Because Defendants knew that a breach of its systems could damage millions of individuals, including Representative Plaintiffs and Class Members, Defendants had a duty to adequately protect those data systems and the PHI/PII and financial information contained thereon.

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

99. Defendants also had independent duties under state and federal laws that required it to reasonably safeguard Representative Plaintiffs' and Class Members' PHI/PII and financial information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendants and Representative Plaintiffs and/or the remaining Class Members.

100. Defendants breached their 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 the PHI/PII and financial information of Representative Plaintiffs and Class Members;

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

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

d. by failing to provide adequate supervision and oversight of the PHI/PII and financial information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third-party to gather PHI/PII and financial

information of Representative Plaintiffs and Class Members, misuse the PHI/ PHI/PII, and intentionally disclose it to others without consent.

e. by failing to adequately train its employees to not store PHI/PII and financial information longer than absolutely necessary;

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

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 financial information and monitor user behavior and activity in order to identify possible threats.

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

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

103. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PHI/PII and financial information 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 and financial information.

104. Defendants breached their duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting months after 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, Defendants have 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.

105. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendants prevented Representative

Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PHI/PII and financial information.

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

107. Defendants' wrongful actions, inactions, and omissions constituted (and continues to constitute) common law negligence.

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

109. 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 Defendants, of failing to use reasonable measures to protect PHI/PII and financial information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

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

111. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PHI/PII and

financial information is used; (iii) the compromise, publication, and/or theft of their PHI/PII and financial information; (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 and financial information; (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) the continued risk to their PHI/PII and financial information, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' PHI/PII and financial information in its continued possession; (vii) and 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 and financial information compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

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

113. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PHI/PII and financial information, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PHI/PII and financial information in its continued possession.

SECOND CLAIM FOR RELIEF
Invasion of Privacy
(On behalf of the Nationwide Class and the New Mexico Subclass)

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

115. Representative Plaintiffs and Class Members had a legitimate expectation of privacy to its PHI/PII and financial information and were entitled to the protection of this information against disclosure to unauthorized third-parties.

116. Defendants owed a duty to Representative Plaintiffs and Class Members to keep their PHI/PII and financial information confidential.

117. Defendants failed to protect and released to unknown and unauthorized third-parties the PHI/PII and financial information of Representative Plaintiffs and Class Members.

118. Defendants allowed unauthorized and unknown third-parties access to and examination of the PHI/PII and financial information of Representative Plaintiffs and Class Members, by way of Defendants' failure to protect the PHI/PII and financial information.

119. The unauthorized release to, custody of, and examination by unauthorized third-parties of the PHI/PII and financial information of Representative Plaintiffs and Class Members is highly offensive to a reasonable person.

120. The unauthorized intrusion was into a place or thing which was private and is entitled to be private. Representative Plaintiffs and Class Members disclosed their PHI/PII and financial information to Defendants as part of obtaining services from Defendants, but privately with an intention that the PHI/PII and financial information would be kept confidential and would be protected from unauthorized disclosure. Representative Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without its authorization.

121. The Data Breach constitutes an intentional interference with Representative Plaintiffs' and Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

122. Defendants 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.

123. Because Defendants 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 Representative Plaintiffs and Class Members.

124. As a proximate result of the above acts and omissions of Defendants, the PHI/PII and financial information of Representative Plaintiffs and Class Members was disclosed to third-parties without authorization, causing Representative Plaintiffs and Class Members to suffer damages.

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

THIRD CLAIM FOR RELIEF
Breach of Confidence
(On behalf of the Nationwide Class and the New Mexico Subclass)

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

127. At all times during Representative Plaintiffs' and Class Members' interactions with Defendants, Defendants were fully aware of the confidential nature of the PHI/PII and financial information that Representative Plaintiffs and Class Members provided to it.

128. As alleged herein and above, Defendants' relationship with Representative Plaintiffs and the Class Members was governed by promises and expectations that Representative Plaintiffs and Class Members' PHI/PII and financial information would be collected, stored, and

protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

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

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

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

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

133. As a direct and proximate cause of Defendants' actions and/or omissions, Representative Plaintiffs and Class Members have suffered damages, as alleged therein.

134. But for Defendants' failure to maintain and protect Representative Plaintiffs' and Class Members' PHI/PII and financial information in violation of the parties' understanding of confidence, its PHI/PII and financial information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third-parties. The Data Breach was the direct and legal cause of the misuse of Representative Plaintiffs' and Class Members' PHI/PII and financial information, as well as the resulting damages.

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

136. As a direct and proximate result of Defendants' breaches of confidence, Representative Plaintiffs and Class Members have suffered and will suffer injury, as alleged herein, including, but not limited to, (a) actual identity theft; (b) the compromise, publication, and/or theft of its PHI/PII and financial information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of its PHI/PII and financial information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to its PHI/PII and financial information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Class Members' PHI/PII and financial information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members; (g) the diminished value of Representative

Plaintiffs' and Class Members' PHI/PII and financial information; and (h) the diminished value of Defendants' services for which Representative Plaintiffs and Class Members paid and received.

FOURTH CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Nationwide Class and the New Mexico Subclass)

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

138. Through its course of conduct, Defendants, Representative Plaintiffs and Class Members entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Representative Plaintiffs' and Class Members' PHI/PII and financial information.

139. Defendants required Representative Plaintiffs and Class Members to provide and entrust their PHI/PII and financial information as a condition of obtaining Defendants' services.

140. Defendants solicited and invited Representative Plaintiffs and Class Members to provide their PHI/PII and financial information as part of Defendants' regular business practices. Representative Plaintiffs and Class Members accepted Defendants' offers and provided their PHI/PII and financial information to Defendants.

141. As a condition of being direct customers/patients/employees of Defendants, Representative Plaintiffs and Class Members provided and entrusted their PHI/PII and financial information to Defendants. In so doing, Representative Plaintiffs and Class Members entered into implied contracts with Defendants by which Defendants 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.

142. A meeting of the minds occurred when Representative Plaintiffs and Class Members agreed to, and did, provide its PHI/PII and financial information to Defendants, in exchange for, amongst other things, the protection of its PHI/PII and financial information.

143. Representative Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

144. Defendants breached the implied contracts it made with Representative Plaintiffs and Class Members by failing to safeguard and protect its PHI/PII and financial information and by failing to provide timely and accurate notice to them that their PHI/PII and financial information was compromised as a result of the Data Breach.

145. As a direct and proximate result of Defendants' above-described breach of implied contract, Representative Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

FIFTH CLAIM FOR RELIEF
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class and the New Mexico Subclass)

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

147. 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.

148. Representative Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendants.

149. Defendants 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 and financial information, failing to timely and accurately disclose the Data Breach to Representative Plaintiffs and Class Members and continued acceptance of PHI/PII and financial

information and storage of other personal information after Defendants knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

150. Defendants 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.

SIXTH CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of the Nationwide Class and the New Mexico Subclass)

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

152. By its wrongful acts and omissions described herein, Defendants have obtained a benefit by unduly taking advantage of Representative Plaintiffs and Class Members.

153. Defendants, prior to and at the time Representative Plaintiffs and Class Members entrusted their PHI/PII and financial information to Defendants for the purpose of obtaining health services, caused Representative Plaintiffs and Class Members to reasonably believe that Defendants would keep such PHI/PII and financial information secure.

154. Defendants was aware, or should have been aware, that reasonable patients and consumers would have wanted their PHI/PII and financial information kept secure and would not have contracted with Defendants, directly or indirectly, had they known that Defendants' information systems were sub-standard for that purpose.

155. Defendants were also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Representative Plaintiffs' and Class Members' decisions to seek services therefrom.

156. Defendants failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Representative Plaintiffs and Class Members made its decisions to make purchases, engage in commerce therewith, and seek services or information. Instead, Defendants suppressed and concealed such information. By concealing and suppressing that information, Defendants denied Representative Plaintiffs and Class Members the

ability to make a rational and informed purchasing and health care decision and took undue advantage of Representative Plaintiffs and Class Members.

157. Defendants was unjustly enriched at the expense of Representative Plaintiffs and Class Members. Defendants received profits, benefits, and compensation, in part, at the expense of Representative Plaintiffs and Class Members. By contrast, Representative Plaintiffs and Class Members did not receive the benefit of their bargain because they paid for products and/or health care services that did not satisfy the purposes for which they bought/sought them.

158. Since Defendants' profits, benefits, and other compensation were obtained by improper means, Defendants are not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

159. Representative Plaintiffs and Class Members seek an Order of this Court requiring Defendants to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendants from its wrongful conduct and/or the establishment of a constructive trust from which Representative Plaintiffs and Class Members may seek restitution.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on behalf of himself/herself/themselves and each member of the proposed National Class and the New Mexico Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendants as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including 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 Defendants, ordering them to cease and desist from unlawful activities;

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

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

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

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

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

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

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

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

k. requiring Defendants 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;

l. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of its 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;

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(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Dated: September 23, 2022

COLE & VAN NOTE

By: */s/ Cody Alexander Bolce*

Cody Bolce, Esq.
California State Bar #322725
COLE & VAN NOTE
555 12th Street, Suite 1725
Oakland, CA 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: cab@colevannote.com

Attorneys for Representative Plaintiffs Deon Nelson and Carol Depriest and the Plaintiffs Class(es)