Daisy Mazoff (Bar No. 028804)
Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: dmazoff@sirillp.com
E: mbarney@sirillp.com
E: tbean@sirillp.com

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Miles Murray, on behalf of himself and all others similarly situated, Plaintiff, v. **Phoenician Medical Center, Inc.** Defendant.	Case No.

CLASS ACTION COMPLAINT

Plaintiff Miles Murray ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against Phoenician Medical Center, Inc. ("Phoenician Medical Center" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Phoenician Medical Center for its failure to properly secure and safeguard Plaintiff's and other similarly situated Phoenician Medical Center patients' personally identifiable information ("PII") and protected health information ("PHI"), including patient names, contact information, state identification, demographic information, date of birth, diagnosis and treatment information, prescription information, medical record numbers, provider name(s), date(s) of service, and health insurance information (the "Private Information"), from criminal hackers.

2. Phoenician Medical Center, based in Phoenix-Valley, is a healthcare corporation that serves tens of thousands of patients.

3. On March 31, 2023, Defendant learned of a data breach concerning its system's servers. In response, Defendant commenced an investigation which revealed that an unauthorized party had access to certain files that contained sensitive patient information (the "Data Breach").

4. On April 25, 2023, Defendant determined that protected health information relating to its current and former patients who were treated between 2016 and 2023 (including Plaintiff and Class Members) may have been accessed and acquired by the unauthorized party.

5. On or about June 30, 2023, Phoenician Medical Center sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

6. Under state and federal law, organizations must report breaches involving protected health information, such as diagnosis and treatment information, prescription information, medical record numbers, provider name(s), date(s) of service, and health insurance information within at least sixty (60) days. Yet, Phoenician Medical Center waited nearly 90 days to notify the public that they were at risk.

7. As a result of this delayed response, Plaintiff and "Class Members" (defined below) had no idea for 3 months that their Private Information had been compromised, and that Plaintiff and Class Members were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, medical diagnosis and treatment information, prescription information, medical record numbers, provider name(s), date(s) of service, and health insurance information that Phoenician Medical Center collected and maintained.

9. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes, including, medical fraud and identity theft by using Class Members' names, health insurance information, and medical record numbers to obtain medical services and/or prescription drugs.

10. There has been no assurance offered by Phoenician Medical Center that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

11. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from medical identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

12. Plaintiff brings this class action lawsuit to address Phoenician Medical Center's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiff and Class

Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals. .

13. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Phoenician Medical Center, and thus Phoenician Medical Center was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

14. Upon information and belief, Phoenician Medical Center and its employees failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had Phoenician Medical Center properly monitored its networks, it would have discovered the Breach sooner.

15. Plaintiff's and Class Members' identities are now at risk because of Phoenician Medical Center's negligent conduct as the Private Information that Phoenician Medical Center collected and maintained is now in the hands of data thieves and other unauthorized third parties.

16. Plaintiff seeks to remedy this harm on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

17. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, negligence *per se*, breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach of confidence, and declaratory/injunctive relief.

II. PARTIES

18. Plaintiff Miles Murray, is, and at all times mentioned herein was, an individual citizen and resident of the State of Arizona.

19. Defendant Phoenician Medical Center is a healthcare corporation incorporated in Arizona, with its principal place of business at 1343 N Alma School Road #160, Chandler, AZ 85224 in Maricopa County.

III. JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Phoenician Medical Center. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has jurisdiction over Phoenician Medical Center because Phoenician Medical Center operates in and/or is incorporated in this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Phoenician Medical Center has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Phoenician Medical Center's Business and Collection of Plaintiff's and Class Members' Private Information

23. Phoenician Medical Center is a healthcare corporation. Founded in 1997, Phoenician Medical Center has over 20+ locations in the United States, serving more than 140,000 patients in Arizona.

24. As a condition of receiving healthcare related services, Phoenician Medical Center requires that its patients entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from Phoenician Medical Center, Plaintiff and Class Members were required to provide their Private Information to Defendant.

25. In its HIPAA Notice of Privacy Practices which, upon information and belief, Phoenician Medical Center presented to all of its patients at the time of receiving healthcare services, promises its patients that it is committed to protecting its patients' personal and medical information and describes the limited specific instances when it shares patient health information with third parties (none of which are applicable here).

26. Thus, due to the highly sensitive and personal nature of the information Phoenician Medical Center acquires and stores with respect to its patients, Phoenician Medical Center, upon information and belief, promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Phoenician Medical Center assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

28. Plaintiff and Class Members relied on Phoenician Medical Center to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiff and Class Members

29. According to Defendant's Notice, it learned of unauthorized access to its computer systems on March 31, 2023.

30. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including contact information, state identification, demographic information, date of birth, diagnosis and treatment information, prescription information, medical record numbers, provider name(s), date(s) of service, and health insurance information.

31. On or about June 30, 2023, roughly 3 months after Phoenician Medical Center learned that the Class's Private Information was first accessed by cybercriminals, Phoenician Medical Center finally began to notify patients that its investigation determined that their Private Information was accessed and acquired.

32. Phoenician Medical Center had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

33. Plaintiff and Class Members provided their Private Information to Phoenician Medical Center with the reasonable expectation and mutual understanding that Phoenician Medical Center would comply with its obligations to keep such Private Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

34. Phoenician Medical Center's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

35. Phoenician Medical Center knew or should have known that its electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

36. Phoenician Medical Center was on notice that companies in the healthcare industry are susceptible targets for data breaches.

37. Phoenician Medical Center was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose

of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[1]

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

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[2]

39. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[3] In 2022, the largest growth in compromises occurred in the healthcare sector.[4]

40. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about

---

[1] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on July 27, 2023).

[2] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on July 27, 2023).

[3] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on July 27, 2023).

[4] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report*, *available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on July 27, 2023).

$20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[5]

41. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[6]

42. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[7]

43. As a healthcare provider, Phoenician Medical Center knew, or should have known, the importance of safeguarding its patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Phoenician Medical Center's patients as a result of a breach. Phoenician Medical Center failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

---

[5] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on July 27, 2023).

[6] *Id.*

[7] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on July 27, 2023).

D. Phoenician Medical Center Failed to Comply with HIPAA

44. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

45. Phoenician Medical Center's Data Breach resulted from a combination of insufficiencies that indicate Phoenician Medical Center failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Phoenician Medical Center's Data Breach that Phoenician Medical Center either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiff's and Class Members' PHI.

46. Plaintiff's and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

47. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

48. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

49. Plaintiff's and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

50. Plaintiff's and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

51. Based upon Defendant's Notice to Plaintiff and Class Members, Phoenician Medical Center reasonably believes that Plaintiff's and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

52. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

53. Phoenician Medical Center reasonably believes that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

54. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

55. Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

56. Phoenician Medical Center reasonably believes that Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

57. It is reasonable to infer that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

58. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

59. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

60. In addition, Phoenician Medical Center's Data Breach could have been prevented if Phoenician Medical Center had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

61. Phoenician Medical Center's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;
b. Failing to mitigate the risks of a data breach and loss of data;
c. Failing to ensure the confidentiality and integrity of electronic protected health information Phoenician Medical Center creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);
d. Failing to implement 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 in violation of 45 CFR 164.312(a)(1);
e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);
f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

62. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required Phoenician Medical Center 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***" (emphasis added).

63. Because Phoenician Medical Center has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to ensure Phoenician Medical Center's approach to information security is adequate and appropriate going forward. Phoenician Medical Center still maintains the PHI and other highly sensitive PII of its current and former patients, including Plaintiff and Class Members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

E. Phoenician Medical Center Failed to Comply with FTC Guidelines

64. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, 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 Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

65. 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 customer 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.

66. The FTC further recommends that companies not maintain PII 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.

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

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

68. As evidenced by the Data Breach, Phoenician Medical Center failed to properly implement basic data security practices. Phoenician Medical Center's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

69. Phoenician Medical Center was at all times fully aware of its obligation to protect the Private Information of its patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Phoenician Medical Center Failed to Comply with Industry Standards

70. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

71. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Phoenician Medical Center include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

72. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems;

and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

73. 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.

74. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

G. Phoenician Medical Center Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

75. In addition to its obligations under federal and state laws, Phoenician Medical Center owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Phoenician Medical Center owed a duty to Plaintiff 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 Private Information of Class Members

76. Phoenician Medical Center breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Phoenician Medical Center's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

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

d. Failing to sufficiently train its employees regarding the proper handling of its patients Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

77. Phoenician Medical Center negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

78. Had Phoenician Medical Center remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

79. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Phoenician Medical Center.

H. Phoenician Medical Center Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

80. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[8] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

81. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

82. Because a person's identity is akin to a puzzle, 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 to otherwise harass or track the victim. 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 individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

[8] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on July 27, 2023).

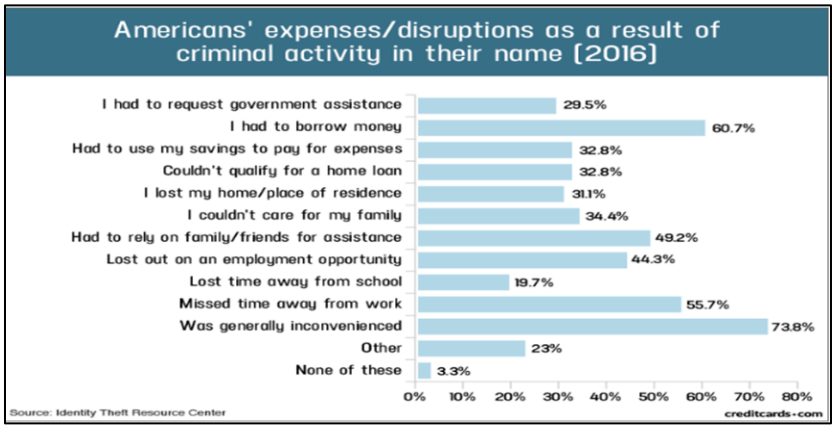
83. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

84. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

85. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[9] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

[9] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited July 27, 2023).

86. In fact, a study by the Identity Theft Resource Center[10] shows the multitude of harms caused by fraudulent use of PII:



87. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[11]

88. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

89. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[12]

90. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim

[10] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on July 27, 2023).

[11] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on July 27, 2023).

[12] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on July 27, 2023).

settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

91. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "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."[13]

92. The ramifications of Phoenician Medical Center's failure to keep its patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

93. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

94. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[14]

> [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

[13] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on July 27, 2023).

[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited July 27, 2023).

> the harm resulting from data breaches cannot necessarily rule out all future harm.

95. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

96. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiff's and Class Members' Damages

Plaintiff Miles Murray's Experience

97. When Plaintiff Murray became a patient and received medical services from Defendant, Defendant required him to provide it with substantial amounts of his PII and PHI.

98. On or about June 30, 2023, Plaintiff Murray received a letter which told him that his Private Information had been accessed and acquired during the Data Breach. The notice letter informed him that the Private Information stolen included his "contact information, state identification, demographic information, date of birth, diagnosis and treatment information, prescription information, medical record number, provider name(s), date(s) of service, and health insurance information."

99. The notice letter offered Plaintiff Murray only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Murray will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

100. Plaintiff Murray suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

101. Plaintiff Murray would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to a data breach.

102. Plaintiff Murray suffered actual injury in the form of having his Private Information compromised and stolen as a result of the Data Breach.

103. Plaintiff Murray suffered actual injury in the form of damages to and diminution in the value of his personal, health, and health insurance information – a form of intangible property that Plaintiff Murray entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

104. Plaintiff Murray suffered imminent and impending injury arising from the substantially increased risk of future medical fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

105. Plaintiff Murray has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

106. As a result of the Data Breach, Plaintiff Murray made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial and insurance accounts/explanations of benefits for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Murray has spent several hours dealing with the Data Breach – valuable time he otherwise would have spent on other activities.

107. As a result of the Data Breach, Plaintiff Murray has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing

cyber and other crimes against him including, but not limited to, fraud and identity theft. Plaintiff Murray is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on his life.

108. Plaintiff Murray also suffered actual injury from having his Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of his PII and PHI, a form of property that Defendant obtained from Plaintiff Murray; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

109. As a result of the Data Breach, Plaintiff Murray anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

110. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

111. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

112. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

113. As a direct and proximate result of Phoenician Medical Center's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, along with other forms of medical or other identity theft.

114. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday

lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and/or closely reviewing and monitoring accounts and credit reports for unauthorized activity for years to come.

115. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

116. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

117. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

118. Plaintiff and Class Members also lost the benefit of the bargain they made with Phoenician Medical Center. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiff and Class Members paid to Phoenician Medical Center (or which was paid on their behalf) was intended to be used by Phoenician Medical Center to fund adequate security of Phoenician Medical Center's system and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class did not receive the benefit of the bargain.

119. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data

brokering industry was worth roughly $200 billion.[15] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to other companies.[16] Consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[17]

120. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

121. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

122. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Phoenician Medical Center, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its

[15] See Data Coup, https://datacoup.com/.
[16] *What is digi.me?*, *DIGI.ME*, https://digi.me/what-is-digime/ (last visited July 27, 2023).
[17] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited July 27, 2023).

patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

123. As a direct and proximate result of Phoenician Medical Center's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

124. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

125. Specifically, Plaintiff proposes the following Nationwide Class, (also referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States whose Private Information was impacted as a result of the Data Breach, including all who were sent a notice of the Data Breach.

126. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

127. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class before the Court determines whether certification is appropriate.

128. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

129. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown

at this time, based on information and belief, the Class consists of tens of thousands of patients of Phoenician Medical Center whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Phoenician Medical Center's records, Class Members' records, publication notice, self-identification, and other means.

130. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Phoenician Medical Center engaged in the conduct alleged herein;

b. Whether Phoenician Medical Center's conduct violated the FTCA and HIPAA;

c. When Phoenician Medical Center learned of the Data Breach

d. Whether Phoenician Medical Center's response to the Data Breach was adequate;

e. Whether Phoenician Medical Center unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Phoenician Medical Center failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Phoenician Medical Center's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Phoenician Medical Center's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Phoenician Medical Center owed a duty to Class Members to safeguard their Private Information;

j. Whether Phoenician Medical Center breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Phoenician Medical Center had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Phoenician Medical Center breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Phoenician Medical Center knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Phoenician Medical Center's misconduct;

p. Whether Phoenician Medical Center's conduct was negligent;

q. Whether Phoenician Medical Center's conduct was *per se* negligent;

r. Whether Phoenician Medical Center was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

131. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class

Members because, *inter alia*, all Class Members were injured through the common misconduct of Phoenician Medical Center. Plaintiff are advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

132. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

133. Predominance. Phoenician Medical Center has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Phoenician Medical Center's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

134. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Phoenician Medical Center. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

135. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Phoenician Medical Center has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

136. Finally, all members of the proposed Class are readily ascertainable. Phoenician Medical Center has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Phoenician Medical Center.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE CLASS)

137. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

138. Phoenician Medical Center knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

139. Phoenician Medical Center's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

140. Phoenician Medical Center knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Phoenician Medical Center was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

141. Phoenician Medical Center owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Phoenician Medical Center's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to HIPAA and FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

142. Phoenician Medical Center's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

143. Phoenician Medical Center's duty also arose because it was bound by industry standards to protect its patients' confidential Private Information.

144. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Phoenician Medical Center owed them a duty of care to not subject them to an unreasonable risk of harm.

145. Phoenician Medical Center, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Phoenician Medical Center's possession.

146. Phoenician Medical Center, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

147. Phoenician Medical Center, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

148. Phoenician Medical Center breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
b. Failing to adequately monitor the security of its networks and systems;
c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;
d. Allowing unauthorized access to Class Members' Private Information;
e. Failing to comply with the FTCA;
f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

149. Phoenician Medical Center acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect himself from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

150. Phoenician Medical Center had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Phoenician Medical Center with their Private Information, including highly sensitive PHI, was predicated on the understanding that Phoenician Medical Center would take adequate security precautions. Moreover, only Phoenician Medical Center had the ability to protect its systems (and the Private Information that it stored on them) from attack.

151. Phoenician Medical Center's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, exfiltrated, and acquired as alleged herein.

152. As a result of Phoenician Medical Center's ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

153. Phoenician Medical Center's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

154. As a result of Phoenician Medical Center's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

155. Phoenician Medical Center also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

156. As a direct and proximate result of Phoenician Medical Center's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

157. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

158. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

159. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Phoenician Medical Center to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE CLASS)

160. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

161. Pursuant to Section 5 of the FTCA, Phoenician Medical Center had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

162. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., Phoenician Medical Center had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

163. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized

individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

164. Phoenician Medical Center breached its duties to Plaintiff and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

165. Specifically, Phoenician Medical Center breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

166. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Phoenician Medical Center's duty in this regard.

167. Phoenician Medical Center also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

168. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Phoenician Medical Center's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

169. Plaintiff and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and Phoenician Medical Center's failure to comply with both constitutes negligence *per se*.

170. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Phoenician Medical Center's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

171. As a direct and proximate result of Phoenician Medical Center's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

172. As a direct and proximate result of Phoenician Medical Center's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

173. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Phoenician Medical Center to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

174. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

175. Plaintiff and Class Members entered into a valid and enforceable contract through which they paid money to Phoenician Medical Center in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information.

176. Phoenician Medical Center's Privacy Policy memorialized the rights and obligations of Phoenician Medical Center and its patients. This document was, upon information and belief, provided to Plaintiff and Class Members in a manner in which it became part of the agreement for services.

177. In the Privacy Policy, Phoenician Medical Center commits to protecting the privacy and security of private information and promises to never share Plaintiff's and Class Members' Private Information except under certain limited circumstances.

178. Plaintiff and Class Members fully performed their obligations under their contracts with Phoenician Medical Center.

179. However, Phoenician Medical Center did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore Phoenician Medical Center breached its contracts with Plaintiff and Class Members.

180. Phoenician Medical Center allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class Members' Private Information without permission. Therefore, Phoenician Medical Center breached the Privacy Policy with Plaintiff and Class Members.

181. Phoenician Medical Center's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in Phoenician Medical Center providing services to Plaintiff and Class Members that were of a diminished value.

182. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiff and Class Members.

183. As a direct and proximate result of Phoenician Medical Center's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

184. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Phoenician Medical Center to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

185. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

186. This Count is pleaded in the alternative to Count III above.

187. Phoenician Medical Center provides healthcare services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for services and/or entrusting their valuable Private Information to Defendant in exchange for such services.

188. Through Defendant's provision of medical services to Plaintiff and Class Members, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Private Information, including PHI, in accordance with its policies, practices, and applicable law.

189. As consideration, Plaintiff and Class Members paid money to Phoenician Medical Center and/or turned over valuable Private Information to Phoenician Medical Center. Accordingly, Plaintiff and Class Members bargained with Phoenician Medical Center to securely maintain and store their Private Information.

190. Phoenician Medical Center accepted payment and/or possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

191. In paying Defendant and/or providing their valuable Private Information to Defendant in exchange for Defendant's services, Plaintiff and Class Members intended and understood that Phoenician Medical Center would adequately safeguard the Private Information as part of those services.

192. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiff's and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

193. Plaintiff and Class Members would not have entrusted their Private Information to Phoenician Medical Center in the absence of such an implied contract.

194. Had Phoenician Medical Center disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to Phoenician Medical Center.

195. As a provider of healthcare, Phoenician Medical Center recognized (or should have recognized) that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the other Class Members.

196. Phoenician Medical Center violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class

Members' Private Information. Phoenician Medical Center further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

197. Additionally, Phoenician Medical Center breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

198. Phoenician Medical Center also breached the implied contracts with Plaintiff and Class Members by failing to implement technical policies and procedures for electronic 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 CFR 164.312(a)(1).

199. Phoenician Medical Center further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

200. Phoenician Medical Center further breached the implied contracts with Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

201. Phoenician Medical Center further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

202. Phoenician Medical Center further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

203. Phoenician Medical Center further breached the implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

204. Phoenician Medical Center further breached the implied contracts with Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

205. Phoenician Medical Center further breached the implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

206. Phoenician Medical Center further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PHI.

207. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide payment and/or accurate and complete Private Information to Phoenician Medical Center in exchange for Phoenician Medical Center's agreement to, *inter alia*, provide services that included protection of their highly sensitive Private Information.

208. Plaintiff and Class Members have been damaged by Phoenician Medical Center's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

209. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

210. This Count is pleaded in the alternative to Counts III and IV above.

211. Plaintiff and Class Members conferred a benefit on Phoenician Medical Center by turning over their Private Information to Defendant and by paying for medical services that should have included cybersecurity protection to protect their Private Information. Plaintiff and Class Members did not receive such protection.

212. Upon information and belief, Phoenician Medical Center funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiff and Class Members.

213. As such, a portion of the payments made by Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Phoenician Medical Center.

214. Phoenician Medical Center has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiff and Class Members (or made on their behalf) that should have been used for adequate cybersecurity practices that it failed to provide.

215. Phoenician Medical Center knew that Plaintiff and Class Members conferred a benefit upon it, which Phoenician Medical Center accepted. Phoenician Medical Center profited from these transactions and the resulting possession and control it had over Plaintiff's and Class Members' Private Information and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments it received therefrom for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

216. If Plaintiff and Class Members had known that Phoenician Medical Center had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

217. Due to Phoenician Medical Center's conduct alleged herein, it would be unjust and inequitable under the circumstances for Phoenician Medical Center to be permitted to retain the benefit of its wrongful conduct.

218. As a direct and proximate result of Phoenician Medical Center's conduct, Plaintiff and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private 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 identity theft; (vi) the continued risk to their Private Information, which remains in Phoenician Medical Center's possession and is subject to further unauthorized disclosures so long as Phoenician Medical Center fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

219. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Phoenician Medical Center and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Phoenician Medical Center from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

220. Plaintiff and Class Members may not have an adequate remedy at law against Phoenician Medical Center, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFF AND THE CLASS)

221. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

222. In light of the special relationship between Phoenician Medical Center and its patients, whereby Phoenician Medical Center became a guardian of Plaintiff's and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI) Phoenician Medical Center was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members. This benefit included (1) the safeguarding of Plaintiff's and Class Members' Private Information; (2) timely notifying Plaintiff and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where Phoenician Medical Center's patients' Private Information was and is stored.

223. Phoenician Medical Center had a fiduciary duty to act for the benefit of Plaintiff and the Class upon matters within the scope of its patients' relationship, in particular to keep the Private Information secure.

224. Phoenician Medical Center breached its fiduciary duties to Plaintiff and Class Members by failing to diligently investigate the Data Breach to determine the number of Class Members affected and notify them within a reasonable and practicable period of time.

225. Phoenician Medical Center breached its fiduciary duties to Plaintiff and the Class by failing to protect their Private Information.

226. Phoenician Medical Center breached its fiduciary duties to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI

Phoenician Medical Center created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

227. Phoenician Medical Center breached its fiduciary duties to Plaintiff and Class Members by 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 CFR 164.312(a)(1).

228. Phoenician Medical Center breached its fiduciary duties to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

229. Phoenician Medical Center breached its fiduciary duties to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

230. Phoenician Medical Center breached its fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

231. Phoenician Medical Center breached its fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

232. Phoenician Medical Center breached its fiduciary duties to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

233. Phoenician Medical Center breached its fiduciary duties to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

234. As a direct and proximate result of Phoenician Medical Center's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

235. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

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

237. Phoenician Medical Center owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

238. Phoenician Medical Center still possesses Private Information regarding Plaintiff and Class Members.

239. Plaintiff alleges that Phoenician Medical Center's data security measures remain inadequate. Furthermore, Plaintiff continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

240. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Phoenician Medical Center owes a legal duty to secure its patients' Private Information and to timely notify customers of a data breach under the common law, HIPAA, and the FTCA;

b. Phoenician Medical Center's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect patients' Private Information; and

c. Phoenician Medical Center continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

241. This Court should also issue corresponding prospective injunctive relief requiring Phoenician Medical Center to employ adequate security protocols consistent with legal and industry standards to protect patients' Private Information, including the following:

a. Order Phoenician Medical Center to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Phoenician Medical Center must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Phoenician Medical Center's systems on a periodic basis, and ordering Phoenician Medical Center to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised,

hackers cannot gain access to other portions of Phoenician Medical Center's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its patients about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

242. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Phoenician Medical Center. The risk of another such breach is real, immediate, and substantial. If another breach at Phoenician Medical Center occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

243. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Phoenician Medical Center if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Phoenician Medical Center's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Phoenician Medical Center has a pre-existing legal obligation to employ such measures.

244. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Phoenician Medical Center, thus preventing future injury to Plaintiff and other patients whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seek the following relief:

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

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

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

d. An order instructing Phoenician Medical Center to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Phoenician Medical Center to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: July 27, 2023

Respectfully submitted,

/s/ Daisy Mazoff

Daisy Mazoff (Bar No. 028804)
Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: dmazoff@sirillp.com
E: mbarney@sirillp.com
E: tbean@sirillp.com

ClassAction.org
