IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

PATRICIA A. DEAN, for herself and on behalf of all others similarly situated, Plaintiff, v. MEDICAL REVIEW INSTITUTE OF AMERICA, LLC and HEALTH CARE SERVICE CORPORATION DBA BLUE CROSS AND BLUE SHIELD OF ILLINOIS, Defendant.	CASE NO.:

CLASS ACTION COMPLAINT

Plaintiff Patricia A. Dean ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendants MEDICAL REVIEW INSTITUTE OF AMERICA, LLC ("MRIoA"), a Utah corporation, and HEALTH CARE SERVICE CORPORATION dba BLUE CROSS AND BLUE SHIELD OF ILLINOIS ("BCBSIL") (collectively, "Defendants"), an Illinois corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out the recent targeted cyberattack against the Medical Review Institute of America ("MRIoA"), a business associate of BCBSIL, to which BCBSIL provided its health plan members' highly confidential data. MRIoA allowed a third party to access its computer systems and data, resulting in the compromise of highly sensitive personal information belonging to hundreds of thousands of persons whose data was sent to MRIoA for

review by BCBSIL (the "Data Breach"). Because of the Data Breach, Plaintiff and thousands of Class Members[1] suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the present and imminent risk of harm caused by the compromise of their sensitive personal information, including Social Security numbers.

2. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to BCBSIL its officials, agents, and affiliated companies, including MRIoA, —was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes demographic information (*i.e.*, first and last name, home address, phone number, email address, and date of birth), Social Security number, clinical information (*i.e.*, medical history/diagnosis/treatment, dates of service, lab test results, prescription information, provider name, medical account number, or anything similar in a medical file and/or record), and health insurance and financial information (*i.e.*, health insurance policy and group plan number, group plan provider, claim information),[2] and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendants collected and maintained (collectively the "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that it

[1] *See* Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/8de68304-84d8-4c9c-bf36-c2de1b461e70.shtml & https://apps.web.maine.gov/online/aeviewer/ME/40/8de68304-84d8-4c9c-bf36-c2de1b461e70.shtml (last visited Jan. 27, 2022).

[2] *See* Notice of Data Breach, Medical Review Institute of America (Jan. 7, 2022), attached hereto as Exhibit A.

collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

5. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on MRIoA's computer system and network in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to the Defendants and thus the Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

6. In addition, MRIoA and its employees failed to properly monitor the computer network and IT systems that housed the Private Information.

7. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.,* opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

10. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

12. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to MRIoA's data security systems, future annual audits, and adequate medical identification and credit monitoring services funded by Defendants.

13. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*; (iii) invasion of privacy; (iv) breach of implied contract, (v) unjust enrichment, and (vi) violation of the Illinois Consumer Fraud and Deceptive and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq*..

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and Plaintiff Patricia A. Dean is a resident of a state (Illinois)

different from the resident state of the principal defendant in this action, Defendant MRIOA (Utah).

15. This Court has personal jurisdiction over Defendant BCBSIL because Defendant BCBSIL is headquartered in this District and Defendant conducts substantial business in Illinois and this District.

16. This Court has personal jurisdiction over Defendant MRIOA because Defendant MRIOA conducts substantial business in Illinois and this District.

17. Venue is proper in this Court pursuant to 28 U.S.C. §1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District and the Plaintiff resides in this District.

PARTIES

18. Plaintiff Patricia A. Dean is, and at all times mentioned herein was, a resident of the State of Illinois residing in Homewood, Illinois, in Cook County. Plaintiff was notified of the Data Breach and her Private Information being compromised upon receiving a data breach notice letter from Defendant MRIoA dated January 7, 2022.[3]

19. Defendant Blues Cross and Blue Shield of Illinois is a division of Health Care Service Corporation, a domestic corporation organized under the laws of the State of Illinois. BCBSIL's principal place of business is located at 300 East Randolph St., Chicago, Illinois, 60601.

20. Defendant Medical Review Institute of America, LLC, is a domestic corporation organized under the laws of the State of Utah with its principal place of business

[3] *See* Exhibit A.

located at 2875 S. Decker Lake Drive Suite 300, Salt Lake City, UT 84119. At least one of the members of the LLC, William W. Low, is a resident of the state of Utah.

DEFENDANT'S BUSINESS

21. Defendant BCBSIL is a division of Health Care Service Corporation, an Illinois corporation. BCBSIL provides and administers health insurance in the state of Illinois.

22. Defendant MRIoA is a business associate of BCBSIL. MRIoA provides external review of medical, dental, behavioral health, pharmacy, vision, disability, workers' compensation, and auto claims for insurance carriers, employers, TPAs, self-administered union groups, pharmacy benefit managers, human resource consultants and departments of insurance throughout the country.[4]

23. MRIoA utilizes a nationwide network of board-certified physician specialists and professionals in over 133 specialties and sub-specialties of medicine. MRIoA has reviewers in most states and has licensed physicians in 50 states, including Illinois.[5]

24. On information and belief, in the ordinary course of providing health insurance, BCBSIL requires its members (including Plaintiff and Class members) to provide sensitive personal and private information such as:

- Demographic information (i.e., first and last name, home address, phone number, email address, and date of birth);
- Social Security number;
- Clinical information (i.e., medical history/diagnosis/treatment, dates of service, lab test results, prescription information, provider name, medical account number, or anything similar in a medical file and/or record), and;
- Financial information;

[4] *See* https://www.mrioa.com/about-us/ (last visited Jan. 27, 2022); *see also* https://www.linkedin.com/company/medical-review-institute-of-america-llc (last visited Jan. 27, 2022).
[5] *See* https://www.linkedin.com/company/medical-review-institute-of-america-llc (last visited Jan. 27, 2022); https://www.mrioa.com/about-us/reviewer-panel/ (last visited Feb. 3, 2022).

BCBSIL also maintains health insurance information (i.e., health insurance policy and group plan number, group plan provider, claim information) relating to members of its plans, including Plaintiff and Class Members.[6]

25. Plaintiff did in fact provide her PII and PHI to Defendant BCBSIL.

26. On information and belief, BCBSIL provided MRIoA with Plaintiff's and Class Members' Private Information to facilitate a clinical peer review of health care services provided to Plaintiff and Class Members.[7]

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

28. On information and belief, BCBSIL provides each of its members (including Plaintiff) with a HIPAA compliant notice titled "HIPPA NOTICE OF PRIVACAY PRACTICES" (the "Privacy Notice") that explains how it handles its members sensitive and confidential information.[8] The Privacy Notice is posted on Defendant's website[9] and, upon information and belief, provided to plan members (including Plaintiff), and is provided to every plan member upon request.[10]

---

[6] *See* Notice of Data Breach, Medical Review Institute of America (Jan. 7, 2022), attached hereto as Exhibit A.
[7] *Id*.
[8] *See* https://www.bcbsil.com/docs/privacy/il/privacy-practices-notice-il.pdf ("Privacy Practices") (last visited Jan. 27, 2022).
[9] *Id*.
[10] *See* https://www.bcbsil.com/legal-and-privacy/privacy-notice-and-forms#:~:text=Blue%20Cross%20and%20Blue%20Shield%20of%20Illinois%20(BCBSIL)%20is%20required,personal%20health%20and%20financial%20information.&text=The%20notice%20tells%20how%20your,can%20be%20used%20or%20disclosed. (last visited Jan. 27, 2022).

29. Because of the highly sensitive and personal nature of the information BCBSIL acquires and stores with respect to its members, BCBSIL promises to, among other things: maintain the privacy and security of protected health care information; and promptly notify its members if a breach occurs which compromises the privacy or security of information.[11]

30. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

31. Plaintiff and the Class Members relied on the Defendants to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE CYBERATTACK

32. On November 9, 2021, MRIoA learned that it was the victim of a sophisticated cyber-attack.[12]

33. After discovering the incident, MRIoA commenced an investigation to determine the full nature and scope of the incident and to secure its network. It also contacted the FBI to inform them of the incident [13]

34. On November 12, 2021, MRIoA found out that the incident involved the unauthorized acquisition of information.[14]

35. The investigation revealed that the Private Information that was accessed without authorization, including the personal information, including health and financial information,

[11] *See* Privacy Practices.
[12] *See* Exhibit A.
[13] *Id*.
[14] *Id*.

Social Security number and demographic information of certain members of BCBSIL, among other clients of MRIoA.[15]

36. Upon information and belief, the Private Information contained in the files accessed by hackers was not encrypted.

37. Upon information and belief, the Data Breach was targeted at MIRoA due to its status as a business associate of healthcare entities and health insurance companies (like BCBSIL) that collect, create, and maintain both PII and PHI.

38. Upon information and belief, the targeted Data Breach was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of the Plaintiff and the Class Members.

39. Because of the Data Breach, data thieves were able to gain access to Defendant MRIoA's IT systems and compromise, and to access and acquire the protected Private Information of Plaintiff and Class Members.

40. What's more, in the notices that MRIoA provided, MRIoA openly admits that the Private Information of Plaintiff and Class Members that was accessed without authorization by hackers was indeed "acquired" by the cyberthieves who perpetrated the Data Breach.[16] This means that not only did the cybercriminals view and access the Private Information without authorization, but they also removed Plaintiff's and Class Members' Private Information from MRIoA's network.

[15] *Id*.
[16] *Id*.

41. Due to Defendant MRIoA's inadequate and insufficient data security measures, Plaintiff and the Class Members now face an increased risk of fraud and identity theft and must deal with that threat forever.

42. Plaintiff believes her Private Information was both stolen in the Data Breach (a fact admitted by MRIoA in its Notice of Data Breach where MRIoA states that the cybercriminals "acquired" the data) and is still in the hands of the hackers. Plaintiff further believes her Private Information was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals who perpetrate cyberattacks of the type that occurred here.

43. Defendants had obligations created by HIPAA, contract, industry standards, common law, and, with respect to BCBSIL, its promises and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

44. Plaintiff and Class Members provided their Private Information to Defendant BCBSIL with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

45. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

46. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[17] Of the 1,862 recorded

[17] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[18] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[19]

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

48. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[20]

49. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[21]

---

[18] *Id*.
[19] *Id*.
[20] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi- secret-service-warn-of-targeted-ransomware (last visited Jan. 25, 2022).
[21] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

50. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the Defendants' industry, including Defendants.

Defendants Fail to Comply with FTC Guidelines

51. 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.

52. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[22]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 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.[23]

53. 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 for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

---

[22] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 15, 2021).

[23] *Id.*

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

56. Defendants failed to properly implement basic data security practices.

57. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

58. Defendants were at all times fully aware of their obligation to protect the PII and PHI of the members of BCBSIL. Defendants were also aware of the significant repercussions that would result from its failure to do so.

Defendant Fail to Comply with Industry Standards

59. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

60. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendant MRIoA, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

61. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

62. Defendant MRIoA 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.

63. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendants' Conduct Violates HIPAA and Evidences Its Insufficient Data Security

64. HIPAA requires covered entities and business associates of covered entities like Defendants to protect against reasonably anticipated threats to the security of sensitive patient health information.

65. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

66. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

67. A Data Breach such as the one Defendants experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

68. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[24]

[24] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4.

69. Defendant MRIoA's Data Breach resulted from a combination of insufficiencies that demonstrate MRIoA and BCBSIL failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANTS' NEGLIGENT ACTS AND BREACHES

70. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect the Private Information of Plaintiff and the Class;

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

d. Failing to train employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to and maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

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

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

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

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

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

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

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

m. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the

members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

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

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

p. Failing to adhere to industry standards for cybersecurity.

71. As the result of antivirus and malware protection software in need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks like the one here, Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing providing unsecured and unencrypted Private Information to MRIoA which in turn allowed cyberthieves to access its IT systems.

72. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant BCBSIL.

Data Breaches Put Consumers at an Increased Risk of Fraud and Identity Theft

73. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[25]

74. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable 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, take over victims' identities in order to engage in illegal financial transactions under the victims' names. 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 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.

75. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent

[25] *See* U.S. Gov. Accounting Office, GAO-07-737, "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" (GOA, 2007). Available at https://www.gao.gov/new.items/d07737.pdf. (last visited Jan. 25, 2022).

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[26]

76. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

77. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

78. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[27]

[26] *See* IdentityTheft.gov, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 25, 2022).

[27] *See* Jason Steele, Credit Card and ID Theft Statistics, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. (last visited Jan. 25, 2022).

79. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[28]

80. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

81. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your

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

insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[29]

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

83. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

84. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

85. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

86. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff

[29] *See* Federal Trade Commission, What to Know About Medical Identity Theft, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft identity-theft (last visited Jan. 25, 2022).

and Class Members are at an increased risk of fraud and identity theft for many years into the future.

87. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

88. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[30] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

89. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[31] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[32]Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

90. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

---

[30] *See* Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 25, 2022).

[31] Identity Theft and Your Social Security Number, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 25, 2022).

[32] *Id*. at 4.

91. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security . number."[33]

92. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[34]

93. Medical information is especially valuable to identity thieves.

94. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[35] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[36]

95. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

96. For this reason, Defendants knew or should have known about these dangers and strengthened their data, IT, and email handling systems accordingly. Defendants were put on

---

[33] Brian Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about- identity-theft (last visited Jan. 25, 2022).

[34] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x- price-of-stolen-credit-card-numbers.html (last visited Jan. 25, 2022).

[35] *See* Omri Toppol, Email Security: How You Are Doing It Wrong & Paying Too Much, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last visited Jan. 25, 2022).

[36] *See* Vaas, Cyberattacks, *supra*, n. 28.

notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

97. To date, Defendants have done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

98. Defendant MRIoA has merely offered Plaintiff and Class Members fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach. What's more, MRIoA places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

99. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

100. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

101. In or around January 7, 2022, Plaintiff received notice from MRIoA that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff's Private Information, including her name, Social Security number, medical treatment information, and health insurance information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed MRIoA's computer system.

102. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not

limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by MRIoA. Plaintiff now spends approximately one hour per day reviewing his bank accounts and other sensitive accounts for irregularities.

103. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including increased anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

104. Subsequent to the Data Breach, Plaintiff experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls and spam emails, all of which appear to be placed with the intent to obtain personal information in order to commit identity theft by way of a social engineering

105. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

106. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

107. 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.

108. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that MRIoA obtained from Plaintiff; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

109. Plaintiff and Class Members were also injured by and suffered benefit-of-the-bargain damages from this Data Breach. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant BCBSIL was intended to be used by Defendant to fund adequate security of Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

110. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses 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 relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

111. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of the Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

CLASS ACTION ALLEGATIONS

112. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

113. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All persons whose Private Information was maintained on MRIoA's system that was compromised in the Data Breach and who were sent a notice of the Data Breach (the "Class").
>
> All members of BCBSIL, whose Private Information was maintained on MRIoA's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "BCBSIL Subclass").

> All Illinois residents whose Private Information was maintained on MRIoA's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Illinois Subclass").

114. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

115. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

116. 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 Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA and the FTC Act;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable injuries as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendant BCBSIL breached implied contracts with Plaintiff and BCBSIL Subclass Members;

l. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendants failed to provide adequate notice of the Data Breach;

n. Whether Defendants violated the Illinois CFA, and;

o. Whether Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages, civil penalties, and/or injunctive relief.

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

118. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

119. Predominance. Defendants have 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 system and unlawfully accessed in the same way. The common issues arising from Defendants' 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.

120. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. 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 Defendants. In contrast, the conduct of 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.

121. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

COUNT ONE

NEGLIGENCE
(On Behalf of Plaintiff and the Subclass against Defendant BCBSIL)

122. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 121 above as if fully set forth herein.

123. Defendant BCBSIL required its members, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of rendering healthcare-related services.

124. Defendant BCBSIL provided the Private Information to Defendant MRIoA for commercial purposes.

125. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant BCBSIL owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft..

126. Defendant BCBSIL owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

127. Defendant BCBSIL's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant BCBSIL and the members of BCBSIL, which is recognized by laws and regulations including but not limited to HIPAA, state law, and common law. Defendant BCBSIL was in a superior position to ensure that its systems

were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

128. Defendant BCBSIL's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

129. In addition, Defendant BCBSIL had a duty to employ reasonable security measures 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.

130. Defendant BCBSIL's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

131. Defendant BCBSIL 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 IT system;

c. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failure to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information; and

f. Failing to adequately notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

132. It was foreseeable that Defendant BCBSIL's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

133. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

134. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

135. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant BCBSIL to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue provide adequate medical identity and credit monitoring to all Class Members.

COUNT TWO

NEGLIGENCE
(On Behalf of Plaintiff and the Class against Defendant MRIoA)

136. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 121 above as if fully set forth herein.

137. HIPAA covered entities of which Defendant MRIoA was and is a business associate (including, without limitation, Defendant BCBSIL) required their members, including Plaintiff and Class Members, to submit non- public Private Information in the ordinary course of rendering healthcare-related services.

138. HIPAA covered entities including Defendant BCBSIL provided this Private Information it required members to provide to Defendant MRIoA for commercial purposes.

139. By accepted the Private Information from the HIPAA covered entities (including Defendant BCBSIL) and by storing this data in its computer property, and sharing it and using it for commercial gain, Defendant MRIoA owed a duty of care to use reasonable means to secure and safeguard its computer property—and Plaintiff's and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft..

140. Defendant MRIoA owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

141. Defendant MRIoA's duty of care to use reasonable security measures arose as a result of the special relationship that existed between its business affiliates, including BCBSIL and AETNA and their members and patients, which is recognized by laws and regulations including but not limited to HIPAA, state law, and common law. Defendant MRIoA was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

142. Defendant MRIoA's duty to use reasonable security measures under HIPAA required Defendant MRIoA to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. §

164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

143. In addition, Defendant MRIoA had a duty to employ reasonable security measures 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.

144. Defendant MRIoA's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

145. Defendant MRIoA 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 IT system;

c. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failure to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information; and

f. Failing to adequately notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

146. It was foreseeable that Defendant MRIoA's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and

Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

147. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

148. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

149. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant MRIoA to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate medical identity and credit monitoring to all Class Members.

COUNT THREE

NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and BCBSIL Subclass Members against Defendant BCBSIL)

150. Plaintiff re-alleges and incorporate by reference Paragraphs 1 through 121 above as if fully set forth herein.

151. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant BCBSIL had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' Private Information.

152. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant BCBSIL had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

153. Pursuant to HIPAA, Defendant BCBSIL had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in

the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

154. Defendant BCBSIL breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act 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.

155. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

156. But for Defendant BCBSIL's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

157. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant BCBSIL's breach of its duties. Defendant BCBSIL knew or should have known that it was failing to meet its duties, and that Defendant BCBSIL's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

159. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant BCBSIL owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft.

Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

COUNT FOUR

NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members against Defendant MRIoA)

160. Plaintiff re-alleges and incorporate by reference Paragraphs 1 through 121 above as if fully set forth herein.

161. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

163. Pursuant to HIPAA, Defendant MRIoA had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

164. Defendant MRIoA breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act 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. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

166. But for Defendant MRIoA's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

167. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant MRIoA's breach of its duties. Defendant MRIoA knew or should have known that it was failing to meet its duties, and that Defendant MRIoA's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

169. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant MRIoA owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

COUNT FIVE

INVASION OF PRIVACY
(On Behalf of Plaintiff and the BCBSIL Subclass against Defendant BCBSIL)

170. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 121 as if fully set forth herein.

171. The State of Illinois recognizes the tort of Invasion of Privacy:

> The elements of the cause of action typically are stated as: (1) the defendant committed an unauthorized intrusion or prying into the plaintiff's seclusion; (2) the intrusion would be highly offensive or objectionable to a reasonable person; (3) the matter intruded on was private; and (4) the intrusion caused the plaintiff anguish and suffering.

Busse v. Motorola, Inc., 351 Ill. App. 3d 67, 71, 813 N.E.2d 1013, 1017 (2004).

172. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant BCBSIL mishandled.

173. Defendant BCBSIL's conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

174. By intentionally failing to keep Plaintiff's and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant BCBSIL intentionally invaded Plaintiff's and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

175. Defendant BCBSIL knew that an ordinary person in Plaintiff's or a Class Member's position would consider Defendant BCBSIL's intentional actions highly offensive and objectionable.

176. Defendant BCBSIL invaded Plaintiff and Class Members' right to privacy and intruded into Plaintiff's and Class Members' seclusion by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

177. Defendant BCBSIL intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

178. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant BCBSIL's conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

179. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant BCBSIL acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

COUNT SIX

INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class against Defendant MRIoA)

180. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 121 as if fully set forth herein.

181. The State of Utah recognizes the tort of Invasion of Privacy:

> The elements of an invasion-of-privacy claim are: (1) the disclosure of the private facts must be a public disclosure and not a private one; (2) the facts disclosed to the public must be private facts, and not public ones; (3) the matter made public must be one that would be highly offensive and objectionable to a reasonable person of ordinary sensibilities.

Shattuck-Owen v. Snowbird Corp, 2000 UT 94, 16 P.3d 555 (2000) (citing *Stien v. Marriott Ownership Resorts, Inc.*, 944 P.2d 374, 380 (Utah Ct.App.1997) (quoting W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 117, at 856-57 (5th ed.1984) (footnote omitted)).

182. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

183. Defendant MRIoA's conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

184. By intentionally failing to keep Plaintiff's and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant MRIoA intentionally invaded Plaintiff's and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

185. Defendant MRIoA knew that an ordinary person in Plaintiff's or a Class Member's position would consider Defendant's intentional actions highly offensive and objectionable.

186. Defendant MRIoA invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' seclusion by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

187. Defendant MRIoA intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

188. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant MRIoA's conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

189. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant MRIoA acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members'

rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

COUNT SEVEN

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the BCBSIL Subclass against Defendant BCBSIL)

190. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 121 as if fully set forth herein.

191. When Plaintiff and Class Members provided their Private Information to BCBSIL in exchange for Defendant BCBSIL's services, they entered into implied contracts with Defendant BCBSIL pursuant to which Defendant BCBSIL agreed to reasonably protect such information.

192. Defendant BCBSIL solicited and invited Class Members to provide their Private Information as part of Defendant BCBSIL's regular business practices. Plaintiff and Class Members accepted Defendant BCBSIL's offer and provided their Private Information to Defendant BCBSIL.

193. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant BCBSIL's data security practices complied with relevant federal and state laws and regulations and were consistent with industry standards.

194. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant BCBSIL include Defendant's promise to protect nonpublic personal information given to Defendant BCBSIL or that Defendant BCBSIL gathers on its own from disclosure.

195. Under these implied contracts, Defendant BCBSIL and/or its affiliated healthcare providers, promised and were obligated to provide healthcare-relates services

including the provision of health insurance, and to maintain the privacy and security of Plaintiff's and Class Members' health care information. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

196. Both the provision of health insurance and the protection of Plaintiff's and Class Members' PII/PHI were material aspects of these implied contracts.

197. At all relevant times, Defendant BCBSIL expressly represented in its Privacy Notice that, among other things, that it would maintain the privacy and security of protected health care information.

198. Defendant BCBSIL's express representations, including, but not limited to, express representations found in its Privacy Notice, memorialized the mutual assent and meeting of the minds between Plaintiff, Class Members, and Defendant BCBSIL, and is part of the implied contract requiring Defendant BCBSIL's to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII/PHI.

199. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII/PHI associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entered into these implied contracts with Defendant BCBSIL and/or its affiliated healthcare providers without an understanding that their PII/PHI would be safeguarded and protected.

200. A meeting of the minds occurred, as Plaintiff and Members of the Class provided their PII/PHI to Defendant BCBSIL and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PII/PHI.

201. Plaintiff and Class Members who paid money to Defendant BCBSIL reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant BCBSIL failed to do so.

202. Plaintiff and Class Members would not have entrusted their Private Information to Defendant BCBSIL in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

203. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant BCBSIL.

204. Through its myriad failures to provide the promised level of data security and protection alleged previously herein, Defendant BCBSIL breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

205. As a direct and proximate result of Defendant BCBSIL's breaches of the implied contracts, Class Members sustained damages as alleged herein.

206. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Thus, Plaintiff and Class Members did not get what they paid for and contractually agreed to.

207. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

208. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate medical identity and credit monitoring to all Class Members.

COUNT EIGHT

UNJUST ENRICHMENT
(On Behalf of Plaintiff and the BCBSIL Subclass against Defendant BCBSIL)

209. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 121 as if fully set forth herein.

210. This count is plead in the alternative to Count Seven (breach of implied contract).

211. Plaintiff and Class Members conferred a monetary benefit on Defendant BCBSIL, by paying Defendant BCBSIL money for health insurance premiums, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII and PHI, and by providing Defendant BCBSIL with their valuable PII and PHI.

212. Defendant BCBSIL enriched itself by saving the costs it reasonably should have expended on hiring a business associate with data security measures that were adequate to secure Plaintiff's and Class Members' PII and PHI, and who would have provided a reasonable level of security that would have prevented the Data Breach.

213. Defendant BCBSIL instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by contracting with a and utilizing a cheaper business associate that employed ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

214. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed

to employ and contract with a business associate that would implement appropriate data management and security measures that are mandated by law and industry standards.

215. Defendant BCBSIL acquired the monetary benefit and PII and PHI through inequitable means in that it failed to disclose that it had hired a business associate with the inadequate security practices previously alleged.

216. If Plaintiff and Class Members knew that Defendant BCBSIL had not secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

217. Plaintiff and Class Members have no adequate remedy at law.

218. As a direct and proximate result of Defendant BCBSIL's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (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 PII and PHI, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI 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 PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

COUNT NINE

Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq*.
(On Behalf of Plaintiff and the Illinois Subclass)

221. Plaintiff and the Illinois Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 121.

222. Plaintiff and the Illinois Subclass are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Illinois Subclass, and Defendants are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

223. Defendants are engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendants engage in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

224. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff's and the Illinois Subclass's sensitive PII and PHI from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials

facts to Plaintiff and the Illinois Subclass regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII and PHI of Plaintiff and the Illinois Subclass; (3) failing to disclose or omitting materials facts to Plaintiff and the Illinois Subclass about Defendants' failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII and PHI of Plaintiff and the Illinois Subclass; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff and the Illinois Subclass's PII and PHI and other personal information from further unauthorized disclosure, release, data breaches, and theft.

225. These actions also constitute deceptive and unfair acts or practices because Defendants knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Illinois Subclass and defeat their reasonable expectations about the security of their PII and PHI.

226. Defendants intended that Plaintiff and the Illinois Subclass rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendants' offering of goods and services.

227. Defendants' wrongful practices were and are injurious to the public because those practices were part of Defendants' generalized course of conduct that applied to the Illinois Subclass. Plaintiff and the Illinois Subclass have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

228. Defendants also violated 815 ILCS 505/2 by failing to promptly and adequately notify Plaintiff and the Illinois Subclass of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

229. As a result of Defendants' wrongful conduct, Plaintiff and the Illinois Subclass were injured in that they never would have provided their PII and PHI to Defendants, or purchased Defendants' services, had they known or been told that Defendants failed to maintain sufficient security to keep their PII and PHI from being hacked and taken and misused by others.

230. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff and the Illinois Subclass have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendants or Defendants' customers that Plaintiff and the Illinois Subclass would not have made had they known of Defendants' inadequate data security; lost control over the value of their PII and PHI; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

231. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the CFA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing

to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three years of medical identity and credit monitoring services for Plaintiff and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: February 3, 2022

Respectfully Submitted,

By: *s/Gary M. Klinger*

Gary M. Klinger
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (202) 975-0477
Email: gklinger@masonllp.com

Gary E. Mason
David K. Lietz
MASON LIETZ & KLINGER LLP
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Telephone: (202) 640.1160
Email:gmason@masaonllp.com
Email:dlietz@masonllp.com

Terrance R. Coates
(pro hac vice forthcoming)
MARKOVITS STOCK & DEMARCO
119 E. Court St.
Cincinnati, OH
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
Email: tcoates@msdlegal.com

Attorneys for Plaintiff and the Proposed Class