IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

SHANE WHITE; AHMED AMER; JOEL THORNTON; PATRICIA A. DEAN; and JAMES BRUNO, individually and on behalf of all others similarly situated, Plaintiffs, v. MEDICAL REVIEW INSTITUTE OF AMERICA, LLC, Defendant.	CASE NO: 2:22-cv-00082 **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Shane White, Ahmed Amer, Joel Thornton, Patricia A. Dean, and James Bruno ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant Medial Review Institute of America, LLC ("MRIoA" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. With this action, Plaintiffs seek to hold Defendant responsible for the harms it caused Plaintiffs and the approximately 134,571 other similarly situated persons ("Class Members") in the massive and preventable ransomware attack that took place on or around November 9, 2021, and in which cyber criminals infiltrated Defendant's inadequately protected network servers where highly sensitive personally identifiable information and protected health information were being kept unprotected ("Data Breach" or "Breach").[1]

[1] *See* https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/DB_-09.09.22.pdf (showing 134,571 individuals affected by the data breach at line 531) (last visited Sep. 30, 2022).

2. Defendant MRIoA, based in Salt Lake City, Utah, advertises itself as "the top medical review company in the United States" and represents that it "takes the privacy and security of [consumer] information very seriously."[2]

3. Defendant MRIoA is a "technology enabled provider of clinical insights to payers and patients through analytics and evidence-based clinical opinions derived from independent specialty reviews and virtual second opinion solutions that empower better decision making."[3]

4. Beginning on or about January 7, 2022, nearly two months after it discovered the Data Breach, Defendant began to notify victims of the Data Breach that the sensitive, non-public information that they had entrusted to it had been accessed and acquired by cybercriminals (the "Notice").

5. According to the Notice letters, the information compromised in the Data Breach includes demographic information (i.e., first and last names, home addresses, phone numbers, email addresses, and dates of birth), Social Security numbers, clinical information (i.e., medical histories/diagnoses/treatments, dates of service, lab test results, prescription information, provider names, medical account numbers, or anything similar in medical files and/or records), and health insurance and financial information (i.e., health insurance policy and group plan numbers, group plan providers, claim information), 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 Defendant collected and maintained (collectively the "Private Information").

[2] https://www.mrioa.com/about-us/compliance/ (last visited Sep. 30, 2022).
[3] *Medical Review Institute of America (MRIoA) Sponsors AMCP Nexus 2021 Annual Conference*, available at, https://www.mrioa.com/medical-review-institute-of-america-sponsors-amcp-nexus-2021-annual-conference/ (last visited Sep. 30, 2022).

6. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

7. Defendant maintained the Private Information in a reckless and negligent 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 Plaintiffs' and Class Members' Private Information was a known risk to Defendant and Defendant was thus on notice that failing to take steps necessary to secure the Private Information from those risks left that information in a dangerous condition.

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

9. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

10. 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.

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

12. Plaintiffs 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.

13. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiffs seek 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 Defendant.

15. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful and negligent conduct, and asserting claims for: (i) negligence, (ii) invasion of privacy; (iii) unjust enrichment, (iv) breach of fiduciary duty; (v) violation of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201, *et seq.*; (vi) violation of the Illinois Consumer Fraud and Deceptive and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq.*; and (vii) violation of the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-1, *et seq*.

PARTIES

16. Plaintiff Shane White is a citizen and resident of the State of Minnesota and received a Notice letter from Defendant dated January 7, 2022, informing him that his Private Information was involved in the Data Breach.

17. Plaintiff Ahmed Amer is a citizen and resident of New Jersey and received a Notice letter from Defendant dated January 20, 2022, informing him that his Private Information was involved in the Data Breach. Defendant has not provided an explanation as to why Plaintiff Amer's letter notifying him of the Data Breach was delayed almost three (3) weeks from when initial Notice letters were sent to victims.

18. Plaintiff Joel Thornton is a resident and citizen of Florida and received a Notice letter from Defendant dated January 7, 2022, informing him that his Private Information was involved in the Data Breach.

19. Plaintiff Patricia A. Dean is a resident and citizen of Illinois and received a Notice letter from Defendant dated January 7, 2022, informing her that her Private Information was involved in the Data Breach.

20. Plaintiff James Bruno is a resident and citizen of Illinois and received a Notice letter from Defendant dated January 7, 2022, informing him that his Private Information was involved in the Data Breach.

21. 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 located at 2875 S. Decker Lake Drive Suite 300, Salt Lake City, UT 84119.

JURISDICTION AND VENUE

22. This 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. Minimal diversity under 28 U.S.C. § 1332(d)(2)(A) is satisfied because the number of class members exceeds 100 and many of whom have different citizenship from all of Defendant's members.

23. This Court has personal jurisdiction over Defendant because it operates in and is headquartered in this District and conducts substantial business in this District.

24. 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. Defendant has its principal place of business in this District, maintains Class Members' Private Information in the District, and has caused harm to Class Members from this District.

FACTUAL ALLEGATIONS

Defendant's Business

25. Defendant 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]

26. To carry out its work, MRIoA utilizes a nationwide network of board-certified physician specialists and professionals in over 150 specialties and sub-specialties of medicine. MRIoA has reviewers in most states and has licensed physicians in 50 states.[5]

[4] *See* https://www.mrioa.com/about-us/; *see also* https://www.linkedin.com/company/medical-review-institute-of-america-llc (last visited Sep. 30, 2022).
[5] *See* https://www.mrioa.com/about-us/reviewer-panel/ (last visited Sep. 30, 2022).

27. On information and belief, in the ordinary course of business, Defendant collects from its customers (including entities to which Plaintiffs and Class Members supplied their Private Information) sensitive personal and non-public 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.

28. Defendant also maintains health insurance information (i.e., health insurance policy and group plan number, group plan provider, claim information) relating to members of its customers' plans, including Plaintiffs and Class Members.

29. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their Private Information confidential and securely maintained, to use this information for business or medical purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their sensitive Private Information.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for and had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties.

The Data Breach

31. According to the Notice letters that Defendant sent to state Attorneys General and Plaintiffs and Class Members, on November 9, 2021, MRIoA learned that it was the victim of a cyber-attack in which an unknown actor accessed and obtained the Private Information of approximately 134,571 individuals.[6] The information obtained by the cyber attackers included at least: demographic information (i.e., first and last name, gender, home address, phone number, email address, date of birth, and 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 similar information in medical files and/or records); and financial information (i.e., health insurance policy and group plan number, group plan provider, claim information).

32. It is evident that the data exposed in the Data Breach was not encrypted because California law requires entities to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1). Defendant notified California residents and the California Attorney General of the Data Breach on or about Feb. 3, 2022, evidencing that the exposed data was unencrypted.

33. Upon information and belief, the cybercriminals who engineered the Data Breach targeted MRIoA due to its status as a business associate of healthcare entities and health insurance companies that collect, create, and maintain Private Information. Moreover, the targeted Data Breach was expressly designed to gain access to private and confidential data, including (among

[6] https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/Data-Breach-year-to-date-Report.pdf (last visited Sep. 30, 2022).

other things) the Private Information of Plaintiffs and the Class Members. Because of Defendant's failure to implement adequate safeguards, data thieves were able to gain access to Defendant's IT systems and to access and acquire the unencrypted Private Information of Plaintiffs and Class Members.

34. In the Notice letter, MRIoA openly admits that the Private Information of Plaintiffs and Class Members was accessed and exfiltrated by hackers. According to Defendant, the Data Breach "involved the unauthorized acquisition of information" and Defendant further claims that "to the best of our ability and knowledge, we retrieved and subsequently confirmed the deletion of the obtained information." But, in recognition of the fact that once exfiltrated from Defendant's network, the Private Information of Plaintiffs and the Class remains at imminent risk of misuse, Defendant admonishes victims of the Data Breach to "remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity." Defendant also offered victims of the Data Breach one year of identity monitoring services, an offer they need not have made if they had actually verified that the Private Information was safe from misuse.

35. A ransomware attack, like the one at issue in this Data Breach, is a type of cyberattack that is frequently used to target healthcare providers due to the sensitive patient data they maintain.[7] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[8] Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in lengthier patient stays, delayed procedures or

[7] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/ (last visited Sep. 30, 2022).
[8] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs (last visited Sep. 30, 2022).

test results, increased complications from surgery, and even increased mortality rates.[9] In 2021, 44% of healthcare providers who experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted services for up to a month.[10]

36. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[11] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."[12]

37. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[13] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[14] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[15] And even where companies pay for the return of data attackers

[9] *Ponemon study finds link between ransomware, increased mortality rate*, available at https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate (last visited Sep. 30, 2022).
[10] *The State of Ransomware in Healthcare 2022*, available at https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf (last visited Sep. 30, 2022).
[11] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last visited Sep. 30, 2022).
[12] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/ (last visited Sep. 30, 2022).
[13] *Id*.
[14] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report (last visited Sep. 30, 2022).
[15] *Id*.

often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[16]

38. Due to MRIoA's inadequate and insufficient data security measures, Plaintiffs and the Class Members now face an increased risk of fraud and identity theft and must deal with that threat forever. Plaintiffs believe their 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 Data Breach "involved the unauthorized acquisition of information") and is still in the hands of the hackers. Plaintiffs further believe that their Private Information was subsequently sold or published 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, and Plaintiffs White and Bruno received alerts that their Private Information was detected on the dark web following the Data Breach.

39. Defendant had obligations created by HIPAA, contracts with the entities that provided it with the Private Information, industry standards, common law, and promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure

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

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

[16] *Id.*

The Data Breach was foreseeable

42. Defendant's 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.

43. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[17] 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.

44. 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.

45. 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

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

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."[18]

46. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[19]

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

Defendant Failed to Comply with FTC Guidelines

48. 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.

49. 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.[20] 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.

---

[18] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[19] *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.

[20] 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.

50. 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.

51. 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 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. These FTC enforcement actions include actions against healthcare-related service providers like the Defendant. 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.")

53. Defendant failed to properly implement basic data security practices.

54. Defendant'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 FTC Act, 15 U.S.C. § 45.

55. Defendant was always fully aware of its obligation to protect the Private Information of Plaintiffs and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

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

57. Several best practices have been identified that at a minimum should be implemented by healthcare service providers and covered business associates like 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.

58. 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.

59. 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.

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

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

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

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

63. 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 Defendant 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).

64. A Data Breach such as the one Defendant 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.

65. 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).[21]

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

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

67. 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."[22]

68. 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,

[21] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4 (last visited Sep. 30, 2022).
[22] *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 Sep. 30, 2022).

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.

69. 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 charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[23]

70. 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.

71. 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

[23] *See* IdentityTheft.gov, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Sep. 30, 2022).

the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

72. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.[24]

73. Moreover, theft of Private Information is also gravely serious. PII and PHI are an extremely valuable property right.[25]

74. 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.

75. Theft of PHI, in particular, is gravely serious. A medical identity thief may use PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care. If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[26]

76. 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

[24] *See, e.g.*, Jason Steele, Credit Card Fraud and ID Theft Statistics, CreditCards.com (June 11, 2021) https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/.

[25] *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).

[26] *See* Federal Trade Commission, What to Know About Medical Identity Theft, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Sep. 30, 2022).

themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

77. 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 is stolen and when it is used.

78. 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.

79. 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.

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

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

82. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[27] PII is particularly valuable because criminals can use it to target victims

[27] 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/.

with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

83. 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.[28] 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.[29] 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.

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

85. 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."[30]

86. 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

[28] Identity Theft and Your Social Security Number, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf .
[29] *Id*. at 4.
[30] 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 Sep. 30, 2022).

information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[31]

87. Medical information is especially valuable to identity thieves.

88. 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.[32] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[33]

89. 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.

90. For this reason, Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Defendant's negligent acts and breaches

91. Defendant breached its obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's 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;

[31] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, Computer World (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sep. 30, 2022).
[32] *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).
[33] *See* Nate Berg, Hackers have figured out how easy it is to take down a hospital, SPLINTER (Mar. 10, 2016, 4:17 PM), http://splinternews.com/hackers-have-figured-out-how-easy-it-is-to-takedown-a-1793855277.

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

c. Failing to properly monitor its 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.

92. 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, Defendant negligently and unlawfully failed to safeguard Plaintiffs' 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.

93. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft.

Plaintiffs' and Class Members' Damages

94. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 12 months of inadequate identity monitoring services, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

95. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, MRIoA places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

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

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

98. Plaintiffs 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.

99. Plaintiffs 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 Plaintiffs and Class Members.

100. Plaintiffs 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.

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

102. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

103. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Cyber-Attack. Moreover, Defendant's delay in notifying affected

persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

104. Plaintiffs 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:

- Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- Purchasing credit monitoring and identity theft prevention;
- Placing "freezes" and "alerts" with reporting agencies;
- 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;
- Contacting financial institutions and closing or modifying financial accounts; and
- Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

105. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, 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.

Plaintiff White's Experience

106. Plaintiff Shane White was an insured individual with Blue Cross and Blue Shield of Minnesota, which provided MRIoA his Private Information "to facilitate a clinical peer review of a health care service [Mr. White] requested or received." Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

107. Plaintiff White received a letter from Defendant dated January 7, 2022, informing him that his Private Information was involved in the Data Breach.

108. As a result of the Data Breach, Defendant directed Plaintiff White to take certain steps to protect his Private Information and otherwise mitigate his damages.

109. As a result of the Data Breach, Plaintiff White has been forced to spend time dealing with the consequences of the Data Breach (self-monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the Notice letter, communicating with his bank, ensuring accounts are locked, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

110. After the Data Breach, Plaintiff White also received a notice from his bank that its identity monitoring service had detected that certain of his Private Information was posted on the dark web.

111. Plaintiff White is very careful about sharing his own Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

112. Plaintiff White stores all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and

financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts to maximize his digital security efforts.

113. Plaintiff White suffered actual injury and damages due to Defendant's mismanagement of his Private Information before and throughout the Data Breach.

114. Plaintiff White suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to Defendant for the purpose of providing healthcare related services, which was compromised in and as a result of the Data Breach.

115. Plaintiff White suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

116. Plaintiff White has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

117. Plaintiff White has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Amer's Experience

118. Plaintiff Ahmed Amer received healthcare related services from an entity that contracted with MRIoA for its services. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

119. Plaintiff Amer received a letter from Defendant dated January 20, 2022, informing him that his Private Information was involved in the Data Breach.

120. As a result of the Data Breach, Defendant directed Plaintiff Amer to take certain steps to protect his Private Information and otherwise mitigate his damages.

121. As a result of the Data Breach, Plaintiff Amer has been forced to spend time dealing with the consequences of the Data Breach (self-monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the Notice letter, communicating with his bank, ensuring accounts are locked, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

122. Plaintiff Amer is very careful about sharing his own Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

123. Plaintiff Amer stores all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts to maximize his digital security efforts.

124. Plaintiff Amer suffered actual injury and damages due to Defendant's mismanagement of his Private Information before and throughout the Data Breach.

125. Plaintiff Amer suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to Defendant for the purpose of providing healthcare related services, which was compromised in and as a result of the Data Breach.

126. Plaintiff Amer suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

127. Plaintiff Amer has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

128. Plaintiff Amer has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Thornton's Experience

129. Plaintiff Thornton received healthcare related services from an entity that contracted with MRIoA for its services. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

130. Plaintiff Thornton received a letter from Defendant dated January 7, 2022, informing him that his Private Information was involved in the Data Breach.

131. As a result of the Data Breach, Defendant directed Plaintiff Thornton to take certain steps to protect his Private Information and otherwise mitigate his damages.

132. As a result of the Data Breach, Plaintiff Thornton has been forced to spend time dealing with the consequences of the Data Breach (self-monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the Notice letter, communicating with his bank, ensuring accounts are locked, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

133. As a result of the Data Breach, Plaintiff Thornton has also paid for and enrolled in additional identity monitoring services including Norton 360, for which he paid $49 per month before upgrading to Norton deluxe and password protector for $98 per month. Plaintiff Thornton

also paid approximately $148 to LifeLock to search for and remove his private information from the dark web.

134. Plaintiff Thornton is very careful about sharing his own Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

135. Plaintiff Thornton stores all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for her various online accounts to maximize his digital security efforts.

136. Plaintiff Thornton suffered actual injury and damages due to Defendant's mismanagement of his Private Information before and throughout the Data Breach.

137. Plaintiff Thornton suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to Defendant for the purpose of providing healthcare related services, which was compromised in and as a result of the Data Breach.

138. Plaintiff Thornton suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

139. Plaintiff Thornton has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

140. Plaintiff Thornton has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Dean's Experience

141. Plaintiff Patricia Dean received healthcare related services from an entity that contracted with MRIoA for its services. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

142. Plaintiff Dean received a letter from Defendant dated January 7, 2022, informing her that her Private Information was involved in the Data Breach.

143. As a result of the Data Breach, Defendant directed Plaintiff Dean to take certain steps to protect her Private Information and otherwise mitigate her damages.

144. As a result of the Data Breach, Plaintiff Dean has been forced to spend time dealing with the consequences of the Data Breach (self-monitoring her bank and credit accounts), as well as her time spent verifying the legitimacy of the Notice letter, communicating with her bank, ensuring accounts are locked, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

145. Plaintiff Dean is very careful about sharing her own Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

146. Plaintiff Dean stores all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and

financial accounts. Moreover, she diligently chooses unique usernames and passwords for his various online accounts to maximize her digital security efforts.

147. Plaintiff Dean suffered actual injury and damages due to Defendant's mismanagement of her Private Information before and throughout the Data Breach.

148. Plaintiff Dean suffered actual injury in the form of damages and diminution in the value of her Private Information—a form of intangible property that she entrusted to Defendant for the purpose of providing healthcare related services, which was compromised in and as a result of the Data Breach.

149. Plaintiff Dean suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

150. Plaintiff Dean has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

151. Plaintiff Dean has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff James Bruno's Experience

152. Plaintiff James Bruno received health insurance an entity that contracted with MRIoA to provide secondary reviews of its denials of insurance claims. MRIoA reviewed his claim following his insurers denial of the same. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

153. Plaintiff Bruno received a letter from Defendant dated January 7, 2022, informing him that his Private Information was involved in the Data Breach.

154. As a result of the Data Breach, Defendant directed Plaintiff Bruno to take certain steps to protect his Private Information and otherwise mitigate his damages.

155. As a result of the Data Breach, Plaintiff Bruno has been forced to spend time dealing with the consequences of the Data Breach (self-monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the Notice letter, communicating with his bank, ensuring accounts are locked, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

156. As a result of the Data Breach, Plaintiff Bruno paid Turbo Tax a one-time fee of $99 for its identity protection service.

157. After the Data Breach, Plaintiff Bruno also received a notice from his bank that its identity monitoring service had detected that certain of his Private Information was posted on the dark web.

158. Plaintiff Bruno has experienced fraudulent charges on his credit cards two times since the Data Breach occurred. Because of these fraudulent charges, Mr. Bruno has had to spend hours obtaining new credit cards and dealing with the ramifications of the fraud.

159. Plaintiff Bruno is very careful about sharing his own Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

160. Plaintiff Bruno stores all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts to maximize his digital security efforts.

161. Plaintiff Bruno suffered actual injury and damages due to Defendant's mismanagement of his Private Information before and throughout the Data Breach.

162. Plaintiff Bruno suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to Defendant for the purpose of providing healthcare related services, which was compromised in and as a result of the Data Breach.

163. Plaintiff Bruno suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

164. Plaintiff Bruno has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information, being placed in the hands of unauthorized third parties and possibly criminals.

165. Plaintiff Bruno has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

166. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

167. Plaintiffs bring this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure 23.

168. Plaintiffs propose the following Class and Subclass definitions, subject to amendment based on information obtained through discovery:

> 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 persons residing in Florida 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 "Florida Subclass");
>
> All persons residing in Illinois 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"); and
>
> All persons residing in New Jersey 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 "New Jersey Subclass").

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

170. Plaintiffs reserve the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

171. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

172. 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 Plaintiffs at this time, based on information and belief, the Class consists of more than 130,000 individuals whose data was compromised in the Data Breach.

173. 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 Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b) Whether Defendant 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 Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d) Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e) Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f) Whether Defendant breached its duty to Class Members to safeguard their Private Information;

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

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

i) Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j) Whether Defendant's conduct was negligent; and

k) Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and injunctive relief.

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

175. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class and have no interests antagonistic to those of other Class Members. Plaintiffs' counsel are competent and experienced in litigating data breach class actions.

176. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data were stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant'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.

177. 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 claim 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 Defendant. 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.

178. Defendant has 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 I

NEGLIGENCE
(On Behalf of Plaintiffs and all Class Members)

179. Plaintiffs re-allege and incorporate by reference each preceding paragraph as if fully set forth herein.

180. Defendant required the submission of Plaintiffs' and Class Members Private Information as a condition of providing healthcare related services for the benefit of Plaintiffs and Class Members. HIPAA covered entities and business associates provided this Private Information to Defendant MRIoA.

181. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information for its own pecuniary benefit and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and disclosed to unauthorized parties.

182. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

183. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the data were wrongfully disclosed.

184. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had 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 and adequate notice to those affected in the case of a data breach.

185. Defendant 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.

186. Defendant also had a duty to use reasonable security measures under HIPAA which 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.

187. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

188. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, including sharing and storing the Private Information of Plaintiffs and Class Members on its computer systems.

189. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and Class Members, the critical importance of providing adequate security of that data, and the necessity for encrypting all data stored on Defendant's systems.

190. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiffs and Class Members, including basic encryption techniques freely available to Defendant.

191. Plaintiffs and Class Members had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

192. Defendant was in a position and able to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

193. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

194. Defendant had a duty to comply with the industry standards set out above.

195. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendant's possession.

196. Defendant, through its actions and omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' Private Information.

197. Defendant, through its actions and omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

198. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised.

199. As a result of Defendant's ongoing failure to notify Plaintiffs and Class Members regarding the type of Private Information that has been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

200. Defendant's breaches of duty caused Plaintiffs and Class Members to suffer from identity theft, fraud, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

201. As a result of Defendant's negligence and breach of duties, Plaintiffs 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.

202. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm,

or risk of imminent harm, suffered by Plaintiffs and Class Members. The Private Information of Plaintiffs and Class Members was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information, by adopting, implementing, and maintaining appropriate security measures.

203. Plaintiffs seek an award of actual damages on behalf of themselves and the Class.

204. In failing to secure Plaintiffs' and Class Members' Private Information and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs, therefore, in addition to seeking actual damages, seek punitive damages on behalf of themselves and the Class.

205. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to consumer information.

COUNT II

INVASION OF PRIVACY
(On Behalf of Plaintiffs and all Class Members)

206. Plaintiffs re-allege and incorporate by reference each preceding paragraph as if fully set forth herein.

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

208. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

209. Defendant intentionally failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted Private Information of Plaintiffs and Class Members.

210. Defendant allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiffs and Class Members, by way of Defendant's failure to protect the Private Information.

211. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and Class Members is highly offensive to a reasonable person.

212. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their Private Information to Defendant as a necessary condition of receiving healthcare or health insurance, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

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

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

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

217. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

COUNT III

UNJUST ENRICHMENT
(On Behalf of Plaintiffs and all Class Members)

218. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

219. Plaintiffs and Class Members conferred a monetary benefit to Defendant when they provided their Private Information and payment to their healthcare or insurance providers, who in turn used a portion of the payment to engage Defendant's services, including Defendant's guardianship of the Private Information.

220. Defendant knew that Plaintiffs and Class Members conferred a monetary benefit to Defendant and it accepted and retained that benefit. Defendant profited from this monetary benefit, as the transmission of Private Information to Defendant from Plaintiffs' and Class Members'

healthcare or insurance providers is an integral part of Defendant's business. Without collecting and maintaining Plaintiffs' and Class Members' Private Information, Defendant would have dramatically diminished business and profits.

221. Defendant was supposed to use some of the monetary benefit provided to it by or on behalf of Plaintiffs and Class Members to secure the Private Information belonging to Plaintiffs and Class Members by paying for costs of adequate data management and security.

222. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiffs and Class Members because Defendant failed to implement necessary security measures to protect the Private Information of Plaintiffs and Class Members.

223. Defendant gained access to the Plaintiffs' and Class Members' Private Information through inequitable means because Defendant failed to disclose that it used inadequate security measures.

224. Plaintiffs and Class Members were unaware of the inadequate security measures and would not have entrusted their Private Information to Defendant had they known of the inadequate security measures.

225. To the extent that this cause of action is pled in the alternative to the others, Plaintiffs and Class Members have no adequate remedy at law.

226. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

227. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

228. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds from the monetary benefit that it unjustly received from them.

COUNT IV

BREACH OF FIDUCIARY DUTY
(On Behalf of all Plaintiffs and all Class Members)

229. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

230. At all relevant times hereto, Defendant owed, and owes, a fiduciary duty to Plaintiffs and the Class, including its duty to keep Plaintiffs' Private Information reasonably secure.

231. The fiduciary duty is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530, which required Defendant to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient information and to secure the health care information it maintains and to keep it free from disclosure.

232. Defendant breached its fiduciary duty to Plaintiff by failing to implement sufficient safeguards and by disclosing Plaintiffs' and other Class members' Private Information to unauthorized third parties.

233. As a direct result of Defendant's breach of its fiduciary duty of confidentiality and the disclosure of Plaintiffs' confidential Private Information, Plaintiffs and the Class members have suffered damages.

234. As a direct result of Defendant's breach of its fiduciary duty and the disclosure of Plaintiffs' and Class members' Private Information, Plaintiffs and the Class have suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, and humiliation.

235. Plaintiffs and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of the PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the

increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; (vii) loss of the benefit of the bargain; and (viii) emotional distress. At the very least, Plaintiffs and the Class are entitled to nominal damages.

COUNT V

VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. § 501.201, *et seq.* (On Behalf of Plaintiff Thornton and the Florida Subclass)

236. Plaintiff Thornton (referred to in this Count as "Plaintiff") re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

237. The FDUTPA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat.§ 501.204.

238. This cause of action is brought pursuant to FDUTPA, which, pursuant to Fla. Stat. § 501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

239. Defendant's offer, provision, and sale of services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§ 501.201-501.213.

240. Plaintiffs and the Florida Subclass members, as "individual[s]," are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. § 501.203(7).

241. Defendant serviced the medical and health insurance information of Plaintiff and the Florida Subclass.

242. Defendant offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

243. Plaintiff and the Florida Subclass members received services from Defendant, primarily for personal purposes.

244. Defendant engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement of medical review services to or for Plaintiff and the Florida Subclass.

245. Defendant's acts, practices, and omissions were done in the course of Defendant's businesses of providing clinical and medical review services throughout Florida and the United States.

246. While engaged in trade or commerce, Defendants violated FDUTPA, including, among other things, by:

a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the Private Information of Plaintiff and Florida Subclass members from unauthorized access and disclosure;

b. Failing to disclose that its computer systems and data security practices were inadequate to safeguard and protect the Private Information from being compromised, stolen, lost, or misused; and

c. Failing to disclose the Healthcare Data Breach to Plaintiff and the Florida Subclass in a timely and accurate manner in violation of Fla. Stat. § 501.171.

247. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

248. Defendant should have disclosed this information because it was in a superior position to know the true facts related to the defective data security.

249. As a direct and proximate result of Defendant's violations of the FDUTPA, Plaintiff and Florida Subclass members have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that Defendant's acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(a).

250. As a direct result of Defendant's knowing violation of the FDUTPA, Plaintiff and the Florida Subclass members are at a substantial present and imminent risk of identity theft. Defendant still possesses Plaintiff's and the Florida Subclass members' Private Information that has been accessed by unauthorized third parties, which is evidence of a substantial and imminent risk of future identity theft for all Plaintiffs and Class Members.

251. Plaintiff and the Florida Subclass members are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, including, but not limited to:

a. ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

b. ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Defendant audit, test, and train security personnel regarding any new or modified procedures;

d. ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering that Defendant purge, delete, and destroy Private Information not necessary for their provisions of services in a reasonably secure manner;

f. ordering that Defendant conduct regular database scans and security checks;

g. ordering that Defendant routinely and continually conduct 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

h. ordering Defendant to meaningfully educate individuals about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps victims should take to protect themselves.

252. Plaintiff brings this action on behalf of himself and the Florida Subclass for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, the Florida Subclass members and the public from Defendant's unfair methods of competition and unfair, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

253. The above unfair, unconscionable, and unlawful practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to

Plaintiff and the Florida Subclass that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

254. Defendant's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

255. Plaintiff and Florida Subclass members seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq*., including, but not limited to, a declaratory judgment that Defendant's actions and/or practices violate the FDUTPA.

256. Plaintiff and Florida Subclass members are also entitled to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

COUNT VI

VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT, 815 Ill. Comp. Stat. § 505/1, *et seq.* ("CFA") (On Behalf of Plaintiffs Dean and Bruno and the Illinois Subclass)

257. Plaintiffs Dean and Bruno (referred to in this Count as "Plaintiffs") re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

258. Plaintiffs bring this claim on behalf of themselves and the Illinois Subclass.

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

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

261. Defendant engaged in deceptive and unfair acts and practices in connection with the sale and advertisement of its services in violation of the CFA, by, inter alia, failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act, soliciting and collecting Plaintiffs' and the Illinois Subclass members' Private Information with knowledge that the information would not be adequately protected, storing Plaintiffs' and Illinois Subclass members' Private Information in an unsecure electronic environment, and failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and the Illinois Subclass's Private Information and other personal information from further unauthorized disclosure, release, and data breaches.

262. Defendant also violated the CFA by failing to timely notify and concealing from Plaintiffs and Illinois Subclass members information regarding the unauthorized release and disclosure of their Private Information. If Plaintiff and Illinois Subclass members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Private Information, medical information, and identities.

263. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its 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 Plaintiffs and the Illinois Subclass and defeat their reasonable expectations about the security of their Private Information.

264. Moreover, Defendant had obligations under HIPAA to maintain the data they collected in a secure manner and endeavor to keep it safe from unauthorized access and exfiltration.

265. Defendant intended that Plaintiffs and the Illinois Subclass, and entities contracting on behalf of Plaintiffs and the Illinois Subclass, rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

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

267. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs 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*.

268. As a result of Defendant's wrongful conduct, Plaintiffs and the Illinois Subclass were injured in that they never would have provided their Private Information to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their Private Information from being hacked and taken and misused by others.

269. As a direct and proximate result of Defendant's violations of the CFA, Plaintiffs 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 Defendant that Plaintiffs and the Illinois Subclass would not have made had they known of Defendant's inadequate data security; lost control over the value of their Private Information; 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 Private Information, entitling them to damages in an amount to be proven at trial.

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

COUNT VII

VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. § 56:8-1, *et seq.* (On Behalf of Plaintiff Amer and the New Jersey Subclass)

271. Plaintiff Amer (referred to in this Count as "Plaintiff") re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

272. Plaintiff and all New Jersey Subclass members are "consumers" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1. 102. The Defendant is a "person" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

273. Defendant's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

274. Defendant advertised, offered, or sold goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of the State of New Jersey.

275. Defendant failed to implement and maintain reasonable security and privacy measures to protect Plaintiff and the New Jersey Subclass members' Personally Identifiable Information in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

276. Defendant failed to provide notice to Plaintiff and the New Jersey Subclass or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

277. Defendant's acts and omissions, as set forth herein, evidence a lack of good faith, honesty in fact and observance of fair dealing, so as to constitute unconscionable commercial practices, in violation of N.J.S.A. 56:8-2.

278. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and the New Jersey Subclass members are required to expend sums to protect and recover their Private Information, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, and thereby suffered ascertainable economic loss.

279. Plaintiff and the New Jersey Subclass members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class and Subclasses;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs 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 Private Information 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 five (5) years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, nominal 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.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

Dated: October 3, 2022

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
Email: gklinger@milberg.com

David K. Lietz (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
Email: dlietz@milberg.com

William B. Federman (admitted *pro hac vice*)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com

Interim Co-Lead Counsel for Plaintiffs

Charles H. Thronson, USB 3260
PARSONS BEHLE & LATIMER
201 S. Main Street, Suite 1800
Salt Lake City, UT 84111
Telephone: (801) 532-1234
Facsimile: (801) 536-6111
CThronson@parsonsbehle.com

Interim Liaison Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on October 3, 2022, a true and correct copy of the foregoing was electronically filed with the Clerk of Court using CM/ECF. Copies of the foregoing document will be served upon interested counsel via transmission of Notices of Electronic Filing generated by CM/ECF.

/s/ Charles H. Thronson
Charles H. Thronson