UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

KIRK BURD, individually and on behalf of all others similarly situated, Plaintiff, v. **OHIO MEDICAL ALLIANCE LLC, d/b/a OHIO MARIJUANA CARD**, Defendant.	**Case No.: 1:25-cv-01779** **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Kirk Burd ("Plaintiff"), on behalf of himself, and all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Ohio Medical Alliance, LLC d/b/a/ Ohio Marijuana Card ("Defendant"). Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII")[1] and Protected Health Information ("PHI") (collectively, "Private Information") that was impacted in a data breach (the "Data Breach" or the "Breach").

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it and its accompanying responsibility to store and transfer that information.

3. Defendant is a provider of telemedicine and in-person services across six states.

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. Recently, it was discovered that an unencrypted and non-password protected database containing 957,434 records belonging to Defendant was exposed.[2] The publicly available database included medical documents indicating patients' diagnosis and the reason they were seeking to be prescribed medical marijuana.[3]

6. Upon information and belief, the following types of Private Information of patients of Defendant were compromised in the Data Breach: names, drivers licenses, addresses, dates of birth, medical records, Social Security numbers, and other internal highly sensitive information.[4]

7. To date, Defendant has yet to provide any notice to impacted patients about the Data Breach.

8. Defendant failed to take precautions designed to keep individuals' Private Information secure.

9. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

---

[2] https://www.websiteplanet.com/news/ohio-medical-alliance-breach-report/ (last visited Aug. 26, 2025).
[3] *Id.*
[4] *Id.*

10. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, Social Security numbers and sensitive medical information that Defendant collected and maintained on behalf of patients.

11. Armed with the Private Information accessed in the Data Breach (and a head start), 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' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, and giving false information to police during an arrest.

12. Additionally, the Private Information compromised can potentially create serious privacy and security risks if placed in the wrong hands. The publicly exposed records contain detailed personal and health information that could potentially be exploited for harassment or extortion attempts. Moreover, marijuana remains illegal under federal law, and medical or recreational marijuana use is something that many people would want to remain private. Similarly, mental health is a deeply private issue that could be stigmatized by employers, friends, or family once publicly exposed.

13. There has been no acknowledgement yet by Defendant that the Data Breach occurred nor any assurances that Defendant is taking steps to protect the Private Information going forward.

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

15. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to affected patients, including Plaintiff and Class Members, of the Breach and the types of information unlawfully accessed.

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

17. Upon information and belief, Defendant failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had Defendant properly monitored its IT Network, it would have discovered the Breach sooner.

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

19. Plaintiff seeks to remedy these harms on behalf of himself, and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

20. Accordingly, Plaintiff, on behalf of himself and the Class, assert claims for negligence, negligence *per se*, unjust enrichment, and breach of implied contract.

PARTIES

Plaintiff

21. Plaintiff is a citizen and resident of Celina, Ohio.

Defendant

22. Defendant Ohio Medical Alliance LLC, d/b/a Ohio Marijuana Card, is a limited liability company incorporated in Ohio, with its headquarters at 4500 Rockside Road,

Independence, OH 44131. It has marijuana doctor office locations located in every major city in Ohio, as well as clinics in Arkansas, Kentucky, Louisiana, Virginia, and West Virginia.

JURISDICTION AND VENUE

23. This Court has 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. The number of class members is more than 100 and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332 (d) (2) (A). Defendant has its principal place of business located in this District.

24. This Court has personal jurisdiction over Defendant because Defendant is registered to do business and maintains its principal place of business in this District.

25. Venue is proper in this Court because Defendant's principal place of business is located in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendant

26. Defendant provides telemedicine and in-person services across six states.

27. As a condition of doing business, Defendant requires that individuals entrust it with highly sensitive personal information. In the ordinary course of receiving services from Defendant, Plaintiff and Class Members were required to provide their Private Information to Defendant.

28. Upon information and belief, Defendant made promises and representations to individuals', including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

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

30. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

31. Recently, it was discovered that an unencrypted and non-password protected database containing 957,434 records belonging to Defendant was exposed.[5] The publicly available database included medical documents indicating patients' diagnosis and the reason they were seeking to be prescribed medical marijuana.[6]

32. Upon information and belief, the following types of Private Information of patients of Defendant were compromised in the Data Breach: names, drivers licenses, addresses, dates of birth, medical records, Social Security numbers, and other internal highly sensitive information.[7]

33. To date, Defendant has yet to provide any notice to impacted patients about the Data Breach.

34. Defendant had obligations created by the FTC Act, HIPPA, contract, common law, and industry standards to keep Plaintiff and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

35. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

---

[5] https://www.websiteplanet.com/news/ohio-medical-alliance-breach-report/ (last visited Aug. 26, 2025).
[6] *Id.*
[7] *Id.*

36. The Data Breach resulted in unauthorized third-party accessing and acquiring files containing unencrypted Private Information of Plaintiff and Class Members. Plaintiff and Class Members' Private Information was accessed and stolen in the Data Breach.

37. Upon information and belief, Plaintiff's Private Information, and that of Class Members, was subsequently published on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

38. Defendant failed to take precautions designed to keep individuals' Private Information secure.

39. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information

40. As a condition to obtain services from Defendant, Plaintiff and Class members were required to give their sensitive and confidential Private Information to Defendant.

41. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class members' Private Information, Defendant would be unable to perform its services.

42. At all relevant times, Defendant knew it was storing sensitive Private Information and that, as a result, its system would be an attractive target for cybercriminals.

43. Defendant also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

44. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class members.

45. Upon information and belief, Defendant made promises to Plaintiff and Class members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

46. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

D. Defendant Knew or Should Have Known of the Risk of a Cyberattack Because Healthcare Entities in Possession of Private Information Are Particularly Suspectable.

47. Data thieves regularly target entities in the healthcare industry like Defendant due to the highly sensitive information that they maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

48. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities like Defendant that collect and store Private Information and other sensitive information, preceding the date of the Data Breach.

49. In light of recent high profile data breaches at other industry-leading companies, including, e.g., Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

50. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[8]

[8] 2024 Data Breach Annual Report, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited Aug. 25, 2025).

51. The 330 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.[9]

52. Entities in custody of PHI and/or medical information reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[10] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[11] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. 40 percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole. [12]

53. Indeed, cyberattacks on medical systems and healthcare and healthcare adjacent companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

54. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from being compromised.

---

[9] *Id.*

[10] *See* Identity Theft Resource Center, 2022 Annual Data Breach Report, https://www.idtheftcenter.org/publication/2022-data-breach-report/ (last visited Aug. 25, 2025).

[11] *See* Elinor Mills, Study: Medical identity theft is costly for victims, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Aug. 25, 2025).

[12] *See id.*

[13] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Aug. 25, 2025).

55. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

56. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

57. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

58. As a healthcare entity in possession of its patients' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

E. Defendant Fails to Comply with FTC Guidelines

59. The FTC has promulgated numerous guides for businesses that 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.

60. In 2016, the FTC updated its publication, *Protecting Personal Information*: *A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[14]

61. 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.[15]

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

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

64. These FTC enforcement actions include actions against healthcare entities that fail to adequately protect patient's data, like 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.").

65. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice

[14] Protecting Personal Information: A Guide for Business, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 25, 2025).
[15] *Id.*

by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

67. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

68. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its patients; Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

F. Defendant Fails to Comply with HIPAA Guidelines

69. Defendant is a covered businesses under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

70. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[16] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

72. HIPAA's *Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

73. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

74. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

75. HIPAA's Security Rule requires Defendant to do the following:

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

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

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

d. Ensure compliance by its workforce.

76. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to

those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

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

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

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

80. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[17] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good

[17] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Aug. 25, 2025).

business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[18]

G. Defendant Fails to Comply with Industry Standards

81. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

82. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendant, 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

83. Other best cybersecurity practices that are standard for employers 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; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

84. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

[18] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Aug. 25, 2025).

85. These foregoing frameworks are existing and applicable industry standards for a business and healthcare provider's obligations to provide adequate data security for its patients' sensitive information. Upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

H. Defendant Owed Plaintiff and Class Members a Duty to Safeguard their Private Information

86. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class members.

87. Defendant owed a duty to Plaintiff and Class members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information

88. Defendant owed a duty to Plaintiff and Class members to implement processes that would detect a compromise of Private Information in a timely manner.

89. Defendant owed a duty to Plaintiff and Class members to act upon data security warnings and alerts in a timely fashion.

90. Defendant owed a duty to Plaintiff and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

91. Defendant owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices.

I. The Data Breach Increases Plaintiff's and Class Members' Risk of Identity Theft

92. The unencrypted Private Information of Plaintiff and Class members has been publicly posted on the dark web leak page, and will end up further disseminated and sold to criminals on the dark web, as that is the *modus operandi* of hackers.

93. Unencrypted Private Information may also fall into the hands of companies that will use the detailed data for targeted marketing without the approval of Plaintiff and Class members.

94. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class members because of the Data Breach.

95. Cyberattacks and data breaches at healthcare companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

96. Researchers have found that among healthcare service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[19]

97. Researchers have further found that at healthcare service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[20]

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

---

[19] *See* Nsikan Akpan, Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks, PBS (Oct. 24, 2019), https://www.pbs.org/newshour /science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.
[20] *See* Sung J. Choi et al., Data Breach Remediation Efforts and Their Implications for Hospital Quality, 54 HEALTH SERVICES RESEARCH 971, 971-980 (2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

99. Plaintiff's and Class members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class members and to profit from their misfortune.

100. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in its possession.

101. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

102. The value of Plaintiff's and the Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years, and criminals frequently post stolen Private Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

103. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

104. One such example of criminals using Private Information for profit is the development of "Fullz" packages.

105. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

106. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

107. Identity thieves can also 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. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

108. Identity thieves can also 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, and/or rent a house or receive medical services in the victim's name.

109. The Social Security Administration has similarly warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[21] 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.[22] 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 because one was already filed on their behalf.

110. Further, 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

[21] *Id.*
[22] *Id. at* 4.

quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

111. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Defendant is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

112. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[24] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[25]

113. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PHI/PII, *they will use it*.[26]

114. Approximately 21% of victims did not realize their identity has been compromised until more than two years after it happened.[27] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[28]

---

[23] 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.

[24] Michael Kan, Here's How Much Your Identity Goes for on the Dark Web, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[25] Dark Web Monitoring: What You Should Know, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[26] *Id.*

[27] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Aug. 15, 2025).

[28] The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages"), EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Aug. 25, 2023).

115. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[29]

116. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

J. Loss of Time to Mitigate the Risk of Identity Theft and Fraud

117. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

118. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class members must monitor their financial accounts for many years to mitigate the risk of identity theft.

119. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

120. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[30]

---

[29] Guide for Assisting Identity Theft Victims, FED. TRADE COMM'N, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[30] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 25, 2025).

121. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[31]

122. And for those Class members who experience actual identity theft and fraud, 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."

K. Diminution of Value of Private Information

123. Private Information is valuable property.[32] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

124. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach is difficult, if not impossible, to change.

125. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit

[31] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited Aug. 25, 2025).
[32] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 25, 2025) ("GAO Report").

card information, personally identifiable information . . . [is] worth more than 10x on the black market."[33]

126. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[34]

127. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[35] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[36] [37] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[38]

128. As a result of the Data Breach, Plaintiff's and Class members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

129. The fraudulent activity resulting from the Data Breach may not come to light for years.

---

[33] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 25, 2025).

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

[35] *See* Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Aug. 25, 2025).

[36] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Aug.25, 2025).

[37] https://datacoup.com/ (last visited Aug. 25, 2025).

[38] https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the, software%20installed%20on%20your%20computer (last visited Aug. 25, 2025).

130. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

131. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to millions of individuals detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

132. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

L. The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

133. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

134. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their Private Information 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.

135. Consequently, Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

136. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor and protect Class members from the risk of identity theft resulting from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class members would not need to bear, but for Defendant's failure to safeguard their Private Information.

M. Loss of the Benefit of the Bargain

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

N. Plaintiff's Experience

138. Plaintiff is a patient of Defendant.

139. As a condition of obtaining services from Defendant, Plaintiff was required to provide Defendant with his Private Information.

140. Defendant was in possession of Plaintiff's Private Information before, during, and after the Data Breach.

141. Plaintiff reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

142. Plaintiff greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff is very concerned about

identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

143. Plaintiff stores any and 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 credit card accounts.

144. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

145. Upon information and belief, as a result of the Data Breach, Plaintiff's Private Information was published on the dark web.

146. As a result of the Data Breach, Plaintiff has spent several hours researching the Data Breach, reviewing his bank accounts, monitoring his credit report, changing his passwords and other necessary mitigation efforts. This is valuable time that Plaintiff would have spent on other activities, including but not limited to work and/or recreation.

147. As a consequence of and following the Data Breach, Plaintiff has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

148. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress.

149. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

151. As a direct and traceable result of the Data Breach, Plaintiff suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit

reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his Private Information; (d) emotional distress because identity thieves now possess his sensitive Private Information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and likely published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff and (g) other economic and non-economic harm.

CLASS ALLEGATIONS

152. Plaintiff brings this class action, individually and on behalf of the following Nationwide Class:

> Nationwide Class: All individuals whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach (the "Class").

153. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

154. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

155. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

156. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Upon information and belief, Plaintiff estimates that the Class is comprised of thousands of members, if not more. The Class is sufficiently numerous to warrant certification.

157. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had her Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and her claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

158. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

159. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

160. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. 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;

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

c. Whether Defendant's storage of Plaintiff and Class Member's Private Information was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff and Class Members' Private Information;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff and Class Members' privacy;

g. Whether Defendant took sufficient steps to individuals' Private Information;

h. Whether Defendant was unjustly enriched; and

i. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

161. Information concerning Defendant's policies is available from Defendant's records.

162. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

163. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

164. Given that Defendant has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

165. Plaintiff restates and realleges all of the allegations stated in paragraphs 1-164, as if fully set forth herein.

166. Defendant knowingly collected, possessed, and maintained Plaintiff and Class Members' Private Information, and therefore had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

167. Defendant's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to

those affected in the case of a cyberattack.

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

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

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

b. To protect the Private Information in its possession it using reasonable and adequate security procedures and systems compliant with industry standards;

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

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

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

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

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

171. Defendant's duty also arose because Defendant was bound by industry standards to protect the confidential Private Information entrusted to it.

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

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

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

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

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

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA and HIPAA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

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

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

178. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff and Class Members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems (and the Private Information that it stored on them) from attack.

179. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

180. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding the Data Breach, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

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

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

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

184. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and

Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

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

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

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

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class

188. Plaintiff restates and realleges all of the allegations stated in paragraphs 1-164, as if fully set forth herein.

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

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

191. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

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

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

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

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

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

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

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

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

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

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

COUNT III
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class)

202. Plaintiff restates and realleges all of the allegations stated in paragraphs 1-164, as if fully set forth herein.

203. Plaintiff and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining medical services from Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for medical services and would not have paid for Defendant's medical services, or would have paid less for them, had they known that Defendant's data security practices were substandard.

204. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

205. Defendant accepted possession of Plaintiff and Class Members' Private Information for the purpose of providing medical services to Plaintiff and Class Members.

206. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

207. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including HIPAA and FTC guidelines on data security) and were consistent with industry standards.

208. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

209. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

210. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relates to the Data Breach.

211. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

212. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

213. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

214. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

215. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

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

217. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

218. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

219. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

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

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

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

222. Plaintiff restates and realleges all of the allegations stated in paragraphs 1-164, as if fully set forth herein.

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

224. Plaintiff and Class Members conferred a benefit on Defendant by providing their Private Information to Defendant. Moreover, upon information and belief, Plaintiff alleges that payments made to Defendant included payment for cybersecurity protection to protect Plaintiff and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiff and Class Members in the form of elevated prices charged by Defendant for its services. Plaintiff and Class Members did not receive such protection.

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

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

227. Defendant has retained the benefits of its unlawful conduct, including the amounts of payment received indirectly from Plaintiff and Class Members that should have been used for

adequate cybersecurity practices that it failed to provide.

228. Defendant knew that Plaintiff and Class Members conferred a benefit upon it, which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiff and Class Members' Private Information and prevented the Data Breach.

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

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

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

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

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

PRAYER FOR RELIEF

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

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

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

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

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: August 26, 2025

Respectfully,

By. */s/ Terence R. Coates*
Terence R. Coates (0085579)
Dylan J. Gould (0097954)
Spencer D. Campbell (0103001)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

David K. Lietz (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015
Phone: 866.252.0878
dlietz@milberg.com

Counsel for Plaintiff and the Proposed Class Members