

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

<p>JULIA SMITH, on behalf of herself individually and on behalf of all others similarly situated,</p> <p style="text-align: center;">Plaintiff,</p> <p style="text-align: center;">v.</p> <p>NORTHEAST ORTHOPEDICS AND SPORTS MEDICINE, PLLC,</p> <p style="text-align: center;">Defendant.</p>	<p>CASE NO. _____</p> <p>CLASS ACTION COMPLAINT</p> <p>JURY DEMAND</p>
---	---

CLASS ACTION COMPLAINT

Plaintiff Julia Smith (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against Defendant Northeast Orthopedics and Sports Medicine, PLLC (“Northeast Orthopedics” or “Defendant”) as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels’ investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach (“Data Breach”) resulting from Northeast Orthopedics’s failure to implement reasonable and industry standard data security practices.

2. Defendant is an “orthopedic practice” that provides healthcare services in “New York and [the] northern New Jersey regions.”¹

3. Plaintiff brings this Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its

¹ <https://neosmteam.com/>

regular business practices, including, but not limited to, names, Social Security numbers, driver's license information, payment information, and dates of birth ("personally identifying information" or "PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

4. Upon information and belief, former and current Defendant patients are required to entrust Defendant with sensitive, non-public Private Information, without which Defendant could not perform its regular business activities, in order to obtain medical services from Defendant. Defendant retains this information for at least many years and even after the patient-physician relationship has ended.

5. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. According to the untitled letter that Defendant sent Plaintiff and other impacted Class Members (the "Notice Letter"), on or about November 22, 2023, Defendant "became aware of unauthorized activity on [its] computer network[.]"² Defendant proceeded to investigate the nature and scope of the suspicious activity and subsequently concluded that "an unauthorized party may have accessed certain files on our network for a limited period of time."³

7. According to the Notice Letter, the compromised Private Information included individuals' names, Social Security numbers, driver's license information, payment information,

² The "Notice Letter". A sample copy is available at <https://apps.web.maine.gov/online/aeviewer/ME/40/c67673f2-5c30-48ba-9d59-2d9a557025cd.shtml>

³ *Id.*

dates of birth, medical record information, health insurance information, and treatment and diagnosis information.⁴

8. Defendant's investigation concluded that the Private Information compromised in the Data Breach included Plaintiff's and approximately 177,000 individuals' information.⁵

9. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect patients' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

10. In breaching their duties to properly safeguard patients' Private Information and give patients timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

11. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and

⁴ *Id.*

⁵ According to the breach report submitted to the Office of the Maine Attorney General, 177,276 persons were impacted in the Data Breach. *See* <https://apps.web.maine.gov/online/aewiewer/ME/40/c67673f2-5c30-48ba-9d59-2d9a557025cd.shtml>

incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

12. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

13. Plaintiff and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (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) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) 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.

14. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

15. Plaintiff Julia Smith is and has been, at all relevant times, a resident and citizen of Dobbs Ferry, New York.

16. Defendant Northeast Orthopedics and Sports Medicine, PLLC is a professional services limited liability company formed under the state laws of New York, with its principal place of business located in Nanuet, New York.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant.⁶ This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

18. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in this District and the computer systems implicated in this Data Breach are likely based in this District. Further, Defendant is authorized to and regularly

⁶ According to the breach report submitted to the Office of the Maine Attorney General, 42 Maine residents were impacted in the Data Breach. *See* <https://apps.web.maine.gov/online/aewiewer/ME/40/c67673f2-5c30-48ba-9d59-2d9a557025cd.shtml>

conducts business in this District and makes decisions regarding corporate governance and management of its businesses in this District, including decisions regarding the security measures to protect its patients' Private Information.

19. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the Data Breach; Defendant's principal place of business is located in this district; Defendant maintains Class Members' Private Information in this District; and Defendant caused harm to Class Members residing in this District.

STATEMENT OF FACTS

Defendant's Business

20. Defendant is an "orthopedic practice" that provides healthcare services in "New York and [the] northern New Jersey regions."⁷

21. Plaintiff and Class Members are current and former patients who obtained medical products and/or services from Defendant.

22. In order to obtain medical services from Defendant, Plaintiff and Class Members were required to provide sensitive and confidential Private Information, including their names, Social Security numbers, and other sensitive information.

23. The information held by Defendant in its computer systems included the unencrypted Private Information of Plaintiff and Class Members.

24. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the Private Information collected from them

⁷ <https://neosmteam.com/>

as a condition of obtaining services at Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

25. Indeed, Defendant provides on its website that: “[w]e adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information, username, password, transaction information and data stored on our Site. Sensitive and private data exchange between the Site and its Users happens over a SSL secured communication channel and is encrypted and protected with digital signatures.”⁸

26. Moreover, upon information and belief, Defendant provides every patient with a HIPAA compliant disclosure form in which it represents that it will protect Plaintiff’s and Class Members’ Private Information.

27. Plaintiff and Class Members provided 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.

28. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

⁸ <https://neosmteam.com/privacy-policy/>

29. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's Private Information safe and confidential.

30. Defendant had obligations created by the FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

31. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

The Data Breach

33. On or about March 5, 2024, Defendant began sending Plaintiff and other victims of the Data Breach an untitled letter (the "Notice Letter"), informing them that:

What Happened? On November 22, 2023, Northeast Orthopedics became aware of unauthorized activity on our computer network and immediately began an investigation with the assistance of third party specialists. On December 29, 2023 the investigation determined an unauthorized party may have accessed certain files on our network for a limited period of time. Therefore, we began a thorough review of the potentially impacted portions of our network to determine the type of information contained therein and to whom the information related. Northeast Orthopedics completed its review on February 8, 2024 and determined information related to you was potentially impacted.

What Information Was Involved? We have determined that the information potentially impacted may have included your name, Social Security number, drivers license

information, payment information, date of birth, medical record information, health insurance information, and treatment and diagnosis information.⁹

34. Omitted from the Notice Letter were the details of the dates of the Data Breach, the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

35. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

36. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was 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.

37. The attacker accessed and acquired files in Defendant’s computer systems containing unencrypted Private Information of Plaintiff and Class Members, including their names, Social Security numbers, PHI and other sensitive information. Plaintiff’s and Class Members’ Private Information was accessed and stolen in the Data Breach.

⁹ Notice Letter.

Data Breaches Are Preventable

38. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹⁰

39. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

¹⁰ See *How to Protect Your Networks from RANSOMWARE*, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Aug. 23, 2021).

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹¹

40. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

¹¹ *Id.* at 3-4.

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].¹²

41. Given that Defendant was storing the sensitive Private Information of its current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

42. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of approximately 177,000 patients, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, & Stores Patients' Private Information

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

¹² See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).

44. Defendant retains and store this information and derive a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform services.

45. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

47. 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.

48. 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.

49. Indeed, Defendant provides on its website that: “[w]e adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information, username, password, transaction information and data stored on our Site. Sensitive and private data exchange between the Site and its Users happens over a SSL secured communication channel and is encrypted and protected with digital signatures.”¹³

¹³ <https://neosmteam.com/privacy-policy/>

50. 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.

Defendant Knew, Or Should Have Known, Of The Risk Because Healthcare Entities In Possession Of Private Information Are Particularly Susceptible To Cyber Attacks

51. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. 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.

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

53. According to the *2023 Annual Data Breach Report*, the number of data compromises in 2023 (3,205) increased by 78 percentage points compared to 2022 (1,801).¹⁴ The ITRC set a new record for the number of data compromises tracked in a year, up 72 percentage points from the previous all-time high in 2021 (1,860).¹⁵

54. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August

¹⁴ <https://www.idtheftcenter.org/publication/2023-data-breach-report/>

¹⁵ *Id.*

2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

55. 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.

56. Additionally, as companies became more dependent on computer systems to run their business,¹⁶ *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹⁷

57. As a custodian of 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, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

58. Indeed, cyber-attacks, such as the one experienced by Defendant, 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, smaller entities that store Private Information are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹⁸

¹⁶<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

¹⁷ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

¹⁸https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

60. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially over one hundred thousand individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

61. 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.

62. 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—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

63. As a healthcare entity in possession of its patients' and former patients' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them 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

[aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection](#) (last accessed Oct. 17, 2022).

and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Private Information

64. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁹ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”²⁰

65. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.²¹ For example, Personal Information can be sold at a price ranging from \$40 to \$200.²² Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²³

66. For example, Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security

¹⁹ 17 C.F.R. § 248.201 (2013).

²⁰ *Id.*

²¹ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Oct. 17, 2022).

²² *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Oct. 17, 2022).

²³ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 21, 2022).

Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²⁴

67. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

68. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[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."²⁵

69. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."²⁶

²⁴ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 17, 2022).

²⁵ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Oct. 17, 2022).

²⁶ *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, available at: <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole->

70. A driver’s license can be a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200.”²⁷

71. According to national credit bureau Experian:

A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

72. According to cybersecurity specialty publication CPO Magazine, “[t]o those unfamiliar with the world of fraud, driver’s license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation.”²⁸ However, this is not the case. As cybersecurity experts point out:

“It’s a gold mine for hackers. With a driver’s license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.”²⁹

73. Victims of driver’s license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.³⁰

customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658 (last visited July 31, 2023).

²⁷ <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658> (last visited on Feb. 21, 2023).

²⁸ <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/> (last visited on Feb. 21, 2023).

²⁹ *Id.*

³⁰ *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021, available at: <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html> (last visited on Feb. 21, 2023).

74. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”³¹

75. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.*, patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient’s complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a “cyber black market” exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

76. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.³² Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.³³ In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.³⁴

³¹ *Medical I.D. Theft*, EFraudPrevention <https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected>. (last visited Nov. 6, 2023).

³² <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/> (last accessed July 24, 2023).

³³ <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed July 24, 2023).

³⁴ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/> (last accessed July 24, 2023).

77. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.³⁵

78. “Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy Forum. “Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief’s activities.”³⁶

79. A study by Experian found that the average cost of medical identity theft is “about \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.³⁷ Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.³⁸

80. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security numbers, names, dates of birth, and PHI.

³⁵ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed July 20, 2021)

³⁶ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/> (last accessed July 24, 2023).

³⁷ See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed July 24, 2023).

³⁸ *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/> (last accessed July 24, 2023).

81. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”³⁹

82. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

83. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁴⁰

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

Defendant Fails To Comply With FTC Guidelines

85. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

³⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Oct. 17, 2022).

⁴⁰ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Oct. 17, 2022).

According to the FTC, the need for data security should be factored into all business decision-making.

86. 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 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.⁴¹

87. 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.⁴²

88. 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.

89. 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

⁴¹ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).

⁴² *Id.*

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.

90. These FTC enforcement actions include actions against healthcare entities, 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.”).

91. 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 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.

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

93. 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.

94. 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.

Defendant Fails To Comply With HIPAA Guidelines

95. Defendant is a covered entity 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.

96. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).⁴³ See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

98. 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.

99. 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.

⁴³ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

100. “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.

101. 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.

102. 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).

103. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information 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.

104. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*”⁴⁴

105. 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).

106. 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 protected health information 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).

107. 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.⁴⁵ The list of resources includes a link to guidelines set by the National Institute of

⁴⁴ Breach Notification Rule, U.S. Dep’t of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

⁴⁵ <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.⁴⁶

Defendant Fails To Comply With Industry Standards

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

109. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, 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.

110. 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; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

⁴⁶ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

111. 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.

112. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and 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.

COMMON INJURIES & DAMAGES

113. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to

undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

The Data Breach Increases Plaintiff's & Class Members' Risk Of Identity Theft

114. The unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers, as already has been experienced by Plaintiff.

115. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

116. 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.

117. 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 off their misfortune.

118. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security

number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

119. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the “mosaic effect.”

120. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of “Fullz” packages.⁴⁷

121. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII 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.

122. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' 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 PII

⁴⁷ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/> (last visited on May 26, 2023).

that was exfiltrated in the Data Breach, criminals may still 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.

123. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

124. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate The Risk Of Identity Theft And Fraud

125. 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 or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

126. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter, instructs Plaintiff and Class Members to take the following measures to protect themselves: “remain vigilant against incidents of identity theft and fraud by reviewing your credit

reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.”⁴⁸

127. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching the Data Breach to verify the incident and obtain more details on its occurrence, locking debit cards, contacting credit bureaus to place locks on their accounts, and monitoring their financial accounts for any unusual activity.

128. 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.”⁴⁹

129. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach 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 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.⁵⁰

130. 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

⁴⁸ Notice Letter.

⁴⁹ 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>.

⁵⁰ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited July 7, 2022).

(“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.”^[4]

Diminution Of Value Of PII and PHI

131. PII and PHI are valuable property rights.⁵¹ Their value is axiomatic, considering the value of Big Data in corporate America and 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.

132. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.⁵²

133. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁵³ 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.^{54,55} Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁵⁶

⁵¹ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Sep. 13, 2022) (“GAO Report”).

⁵² 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).

⁵³ 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 Sep. 13, 2022).

⁵⁴ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

⁵⁵ <https://datacoup.com/>

⁵⁶ <https://digi.me/what-is-digime/>

134. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”⁵⁷

135. 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.

136. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

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

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

⁵⁷ *Medical I.D. Theft*, EFraudPrevention <https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected>. (last visited Nov. 6, 2023).

139. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendants network, amounting to potentially over one hundred thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

140. 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.

Future Cost Of Credit And Identity Theft Monitoring Is Reasonable And Necessary

141. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, 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.

142. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her 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.

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

144. 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 to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

145. 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 medical services, Plaintiff and other reasonable consumers 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.

PLAINTIFF SMITH'S EXPERIENCE

146. Plaintiff Smith is a former patient at Defendant who obtained services there in approximately 2018.

147. As a condition of obtaining services at Defendant, she was required to provide her sensitive Private Information to Defendant, including her name, date of birth, Social Security number, and other sensitive information.

148. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Smith's Private Information in its system.

149. Plaintiff Smith is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

150. Plaintiff Smith received the Notice Letter, by U.S. mail, directly from Defendant, dated March 5, 2024, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including her name, Social Security number, drivers license information, payment information, date of birth, medical record information, health insurance information, and treatment and diagnosis information.

151. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff to “remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors[,]”⁵⁸ Plaintiff Smith made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach to verify the incident and obtain more details on its occurrence, locking debit cards, contacting credit bureaus to place locks on their accounts, and monitoring their financial accounts for any unusual activity. Plaintiff has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

152. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her 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) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a)

⁵⁸ Notice Letter.

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.

153. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

154. The Data Breach has caused Plaintiff Smith to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

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

156. As a result of the Data Breach, Plaintiff Smith is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

157. Plaintiff Smith 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.

CLASS ACTION ALLEGATIONS

158. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

159. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All persons whose Private Information was maintained on Defendant's computer systems that were compromised in the Data Breach reported by Defendant in March 2024 (the "Class").

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

161. Plaintiff hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

162. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists at least 177,000 persons whose data was compromised in Data Breach.⁵⁹

163. 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 Plaintiff's 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;

⁵⁹ <https://apps.web.maine.gov/online/aewiewer/ME/40/c67673f2-5c30-48ba-9d59-2d9a557025cd.shtml>

- 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 Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant breached implied contracts for adequate data security with Plaintiff and Class Members;
- l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiff and Class Members;
- m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,
- n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

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

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

166. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' Private Information was 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.

167. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for 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.

168. 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.

169. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and
- e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

170. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Defendant.

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

171. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

172. Defendant requires its patients, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing its medical services.

173. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

174. Plaintiff and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

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

176. 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 their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

177. 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.

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

179. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiff or Class Members of the Data Breach until March 5, 2024 despite, upon information and belief, Defendant knowing shortly after November 22, 2023 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiff and the Class.

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

181. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of being patients of Defendant.

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

183. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

184. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information it was no longer required to retain pursuant to regulations.

185. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

186. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class 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 Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

187. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;

- c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- f. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations, and
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

188. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. 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.

189. Plaintiff and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

190. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

191. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

192. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

193. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

195. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

196. Plaintiff and the Class 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 Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

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

198. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

199. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

200. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

201. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

202. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

203. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost 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.

204. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, 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) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) 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.

205. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

206. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of 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 in its continued possession.

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

208. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

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

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

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

210. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

211. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of receiving medical services from Defendant.

212. 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.

213. 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.

214. 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.

215. Defendant solicited, offered, and invited Plaintiff and 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.

216. In accepting the Private Information of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

217. 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 relate to the Data Breach.

218. 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.

219. 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 and were consistent with industry standards.

220. 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.

221. 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.

222. 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.

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

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

225. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

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

THIRD COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

227. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

228. Plaintiff brings this claim in the alternative to the breach of implied contract claim above.

229. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

230. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving services at Defendant. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

231. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

232. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

233. Defendant, however, failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

234. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

235. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

236. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

237. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

238. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

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

240. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, 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) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) 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.

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

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

FOURTH COUNT
VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT ("GBL")
(New York Gen. Bus. Law § 349)
(On Behalf of Plaintiff and All Class Members)

243. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

244. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including, but not limited to, the following:

- a. Misrepresenting material facts to Plaintiff and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Private Information;
- c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' Private Information;
- d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,
- e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

245. Defendant knew or should have known that its network and data security practices were inadequate to safeguard the Class Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

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

247. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of Defendant's network and aggregation of Private Information.

248. The representations upon which current and former patients (including Plaintiff and some Class Members) relied were material representations (e.g., as to Defendant's adequate protection of Private Information), and current and former patients relied on those representations to their detriment.

249. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

250. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' Private Information and that the risk of a data security incident was high.

251. Defendant's acts, practices, and omissions were done in the course of Defendant's business of furnishing employment benefit services to consumers in the State of New York.

252. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages.

253. Plaintiff and Class Members were injured because:

- a) Plaintiff and Class Members would not have paid Defendant for services had they known the true nature and character of Defendant's data security practices;
- b) Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and
- c) Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

254. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiff and the Class Members suffered 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) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) 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.

255. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

256. Plaintiff brings this action on behalf of herself and Class Members 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, Class Members and the public from Defendant's unfair, deceptive, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

257. Plaintiff seeks relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

258. On behalf of herself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover her actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent 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 Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- ix. requiring Defendant to conduct regular database scanning and securing checks;
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate

- based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
 - xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
 - xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
 - xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
 - xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

- xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;
- E. For an award of punitive damages, as allowable by law;
- F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;
- G. Pre- and post-judgment interest on any amounts awarded; and
- H. Such other and further relief as this court may deem just and proper.

Dated: March 15, 2024

Respectfully submitted,

/s/ Vicki J. Maniatis

Vicki J. Maniatis, Esq.

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN PLLC

100 Garden City Plaza, Suite 500

Garden City, New York 11530

Phone: (865) 412-2700

vmaniatis@milberg.com

David K. Lietz*

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

dlietz@milberg.com

**Pro Hac Vice Application Forthcoming
Counsel for Plaintiff and the Proposed Class*

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Alleges Northeast Orthopedics Left Patient Info Vulnerable to Data Breach](#)
