SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF BRONX

----------X

MARILYN RIVERA, on behalf of herself and all others similarly situated, FRANCHIE MUNIZ, on behalf of himself and all others similarly situated, MICHELLE OWENS, individually and on behalf of all others similarly situated, FLORIN CARSTENOIU, individually and on behalf of all others similarly situated, LUIGI HERNANDEZ, and ANGGIE GENAO DE HERNANDEZ, on behalf of all others similarly situated,

Plaintiffs,

-against-

ESSEN MEDICAL ASSOCIATES, P.C. d/b/a ESSEN HEALTH CARE,

Defendant.

----------X

Index No.: 801239/2024E

CONSOLIDATED CLASS ACTION COMPLAINT

JURY DEMAND

Plaintiffs Marilyn Rivera, Franchie Muniz, Michelle Owens, Florin Carstenoiu, Luigi Hernandez, and Anggie Genao De Hernandez ("Plaintiffs") bring this Consolidated Class Action Complaint ("Complaint") against Defendant Essen Medical Associates, P.C. d/b/a Essen Health Care ("Essen" or "Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their 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 Defendant's failure to implement reasonable and industry standard data security practices.

2. Defendant Essen is a New York-based healthcare provider that offers medical products and services to its patients.

3. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Plaintiffs' and Class Members' sensitive information, including their full names, driver's license or state identification numbers, U.S. Alien Registration numbers, non-U.S. identification numbers, passport numbers, financial account information, dates of birth, Social Security numbers ("personally identifiable information" or "PII") and medical treatment and insurance information, which is protected health information ("PHI" and collectively, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, "Private Information").

4. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cybercriminals who target Private Information for its value to identity thieves.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Essen's patients' Private Information from a foreseeable and preventable cyberattack.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer networks in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Defendant disregarded the rights of Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs 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.

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

9. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, e.g., opening new financial accounts in Plaintiffs' and Class Members' names, taking out loans in Plaintiffs' and Class Members' names, using Plaintiffs' and Class Members' information to obtain government benefits, filing fraudulent tax returns using Plaintiffs' and Class Members' information, obtaining driver's licenses in Plaintiffs' and Class Members' names but with another person's photograph, and giving false information to police during an arrest.

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

11. Plaintiffs and Class Members have suffered injury 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 associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) Plaintiffs' Private Information being disseminated on the dark web; (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.

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

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

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

15. Plaintiffs seek remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

16. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct.

PARTIES

17. Plaintiff Marilyn Rivera is and has been, at all relevant times, a resident and citizen of New York.

18. Plaintiff Franchie Muniz is and has been, at all relevant times, a resident and citizen of New York.

19. Plaintiff Michelle Owens is and has been, at all relevant times, a resident and citizen of New York.

20. Plaintiff Florin Carstenoiu is and has been, at all relevant times, a resident and citizen of New York.

21. Plaintiff Luigi Hernandez is and has been, at all relevant times, a resident and citizen of New York.

22. Plaintiff Anggie Genao De Hernandez is and has been, at all relevant times, a resident and citizen of New York.

23. Defendant Essen Medical Associates, P.C. d/b/a Essen Health Care is a New York-based corporation with its principal place of business located in Bronx, New York.

JURISDICTION AND VENUE

24. This Court has personal jurisdiction over Defendant because it conducts business within the State of New York and this judicial district.

25. Venue is proper in this Court pursuant to CPLR § 503 because Defendant regularly advertises and markets its services and conducts business and because a substantial part of the events or omissions giving rise to the claims occurred in Bronx, New York.

BACKGROUND

Defendant's Business

26. Defendant Essen is a New York-based healthcare provider that offers medical products and services to its patients.

27. Plaintiffs and Class Members are current and former patients of Essen.

28. As a condition of receiving medical services at Essen, Essen requires that its patients, including Plaintiffs and Class Members, entrust Defendant with highly sensitive personal information.

29. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

30. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiffs and Class Members, that the Private Information collected from them as a condition of obtaining medical services at Essen 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.

31. Indeed, on its website, Essen provides that: "[t]o prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic and managerial procedures to safeguard and secure the information we collect through our Websites."[1]

[1] Essen Health Care, *Privacy Policy*, https://essenhealthcare.com/privacy-policy/ (last visited Mar. 22, 2024).

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

33. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs 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. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

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

35. Defendant had obligations created by the Federal Trade Commission Act ("FTC Act"), HIPAA, contract, industry standards, and representations made to patients, to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

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

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

The Data Breach

38. On or about December 29, 2023, Essen began sending Plaintiffs and other victims of the Data Breach a Notice of Incident letter (the "Notice Letter"), informing them that:

> **What Happened.** On March 17, 2023, Essen learned that an unauthorized actor may have accessed its systems and obtained a limited amount of system information. The electronic health record system that Essen uses for storage of medical records was not affected. Upon discovering this incident, we immediately took steps to contain the incident. We then launched an investigation with the assistance of third-party cybersecurity specialists to determine the nature and scope of the incident. We also notified federal law enforcement. The investigation found that an unauthorized actor accessed certain Essen systems between March 14, 2023, and March 22, 2023, and may have accessed or copied certain information maintained within the Essen environment. Essen reviewed the data to understand what type of information it contained and to whom it related. Essen recently completed this review and confirmed that personal information and/or PHI relating to certain individuals was affected by this incident.
>
> **What Information Was Affected.** The information included in the affected files varied by individual, and contained, as applicable, individuals' names, Social Security number, driver's license or state identification number, US Alien Registration number, non-US identification number, passport number, date of birth, diagnosis, financial account information, health insurance information, lab results, medical history, medical record number, medical treatment, patient account number, patient identification number, physician, and/or prescription information.[2]

39. Omitted from the Notice Letter were the details of 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 Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

40. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without

[2] Essen Health Care, *Notice of Data Privacy Event*, https://essenhealthcare.com/wp-content/uploads/2024/01/NOTICE-OF-DATA-PRIVACY-EVENT.pdf (last visited Mar. 22, 2024).

these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

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

42. The cybercriminals that obtained Plaintiffs' and Class members' PII/PHI appear to be the cybercriminal group "BlackCat/ALPHV."[3] Specifically, on May 4, 2023, ALPHV/BlackCat posted on its leak site that it had 24 stolen files from Essen Medical.[4]

43. ALPHV Blackcat is an especially notorious cybercriminal group. In fact, the Federal Bureau of Investigation ("FBI") and the Cybersecurity and Infrastructure Security Agency ("CISA") released a joint report warning the public about ALPHV Blackcat.[5] Specifically, the joint "Cybersecurity Advisory" ("CSA") stated, inter alia, that:

a. "ALPHV Blackcat actors released a new version of the malware, and the FBI identified over 1000 victims worldwide targeted via ransomware and/or data extortion."[6]

b. "This ALPHV Blackcat update has the capability to encrypt both Windows and Linux devices, and VMWare instances."[7]

[3] https://thecyberexpress.com/constellation-software-cyber-attack-alphv-gang/ (last accessed Mar. 21, 2024).
[4] *Id.*
[5] https://www.cisa.gov/sites/default/files/2023-12/aa23-353a-stopransomware-alphv-blackcat_0.pdf (last accessed Mar. 21, 2024).
[6] https://www.aha.org/cybersecurity-government-intelligence-reports/2023-12-19-joint-cybersecurity-advisory-tlp-clear-stopransomware-alphv-blackcat (last accessed Mar. 22, 2024).
[7] *Supra* note 5.

c. "ALPHV Blackcat affiliates have extensive networks and experience with ransomware and data extortion operations."[8]

d. "According to the FBI, as of September 2023, ALPHV Blackcat affiliates have compromised over 1000 entities—nearly 75 percent of which are in the United States and approximately 250 outside the United States—, demanded over $500 million, and received nearly $300 million in ransom payments."[9]

e. "ALPHV Blackcat affiliates use advanced social engineering techniques and open-source research on a company to gain initial access."[10]

f. "Some ALPHV Blackcat affiliates exfiltrate data after gaining access and extort victims without deploying ransomware. After exfiltrating and/or encrypting data, ALPHV Blackcat affiliates communicate with victims via TOR, Tox, email, or encrypted applications."[11]

44. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[12]

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

---

[8] *Id.*
[9] *Supra* note 6.
[10] *Supra* note 5.
[11] *Id.*
[12] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

46. Plaintiff Rivera has been informed that her Private Information has been disseminated on the dark web, and thus Plaintiffs further believe that their Private Information and that of Class Members was or will be sold on the dark web, as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

Data Breaches Are Preventable

47. 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."[13]

48. To prevent and detect cyberattacks 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.

[13] How to Protect Your Networks from RANSOMWARE, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Mar. 22, 2024)

- 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 written access to those files, directories, or shares.

- 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.[14]

49. To prevent and detect cyberattacks 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;

[14] *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].[15]

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

51. 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 PII of, upon information and belief, thousands of individuals, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores Patients' Private Information

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

[15] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

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

54. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

55. Plaintiffs 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.

56. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

57. Defendant's negligence in safeguarding the Private Information of Plaintiffs 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 Cyberattacks.

58. 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.

59. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the breach.

60. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' Personal Information being compromised.[16]

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

62. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential.

63. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[17] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the patients were

[16] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Mar. 22, 2024).
[17] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impacts the economy as a whole.[18]

64. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

65. Indeed, cyberattacks, such as the one experienced by Defendant, have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, 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."[19]

66. Additionally, as companies became more dependent on computer systems to run their businesses,[20] the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[21]

67. 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 Plaintiffs and Class Members from being compromised.

---

[18] *See id.*

[19] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomeware*, Law350 (Nov. 18, 2019, 9:44 PM), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection.

[20] Danny Brando, et al, *Implications of Cyber Risk for Financial Stability*, Board of Governors of the Federal Reserve System (May 12, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.

[21] Dr. Suleyman Ozarslan, *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, Picus, (Mar. 24, 2022), https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.

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

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

70. The injuries to Plaintiffs 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 Plaintiffs and Class Members.

71. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs 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.

72. 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 Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems, or those on which they transferred Private Information, were breached. This includes the significant costs imposed on Plaintiffs 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

73. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[22] 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."[23]

74. 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.[24]

75. For example, Personal Information can be sold at a price ranging from $40 to $200.[25] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[26]

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

---

[22] 17 C.F.R. § 248.201 (2013).
[23] *Id.*
[24] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends,) Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[25] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[26] *In the Dark*, VPNOverview, (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

> 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.[27]

77. 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.

78. 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."[28]

79. Driver's license numbers, which were also compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[29]

---

[27] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf.
[28] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.
[29] Lee Mathews, *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, (Apr. 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658.

80. A driver's license can be a critical part of a fraudulent, synthetic identity—which goes for about $1200 on the dark web. On its own, a forged license can sell for around $200."[30]

81. 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.

82. 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."[31] 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."[32]

83. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent *New York Times* article.[33]

---

[30] *Id.*
[31] Scott Ikeda, Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims, CPO Magazine (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/.
[32] *Id.*
[33] *How Identity Thieves Took My Wife for a Ride,* NY Times (April 27, 2021), https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html. (last visited on Feb. 21, 2023).

84. Theft of PHI is 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."[34]

85. According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.[35]

86. 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 number, date of birth, PHI, and name.

87. This data demands a much higher price on the black market. Rivera 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."[36]

88. 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.

---

[34] eFraud Prevention, Medical I.D. Theft, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected. (last accessed Mar. 22. 2024).
[35] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://news.sophos.com/en-us/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/.
[36] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

89. 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.[37]

90. Plaintiffs 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

91. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

92. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity 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.[38]

---

[37] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

[38] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

93. 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.[39]

94. 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.

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

96. 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. (Essen) ¶ 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.").

97. 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

[39] *Id.*

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

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

99. Upon information and belief, Defendant was at all times fully aware of its obligations 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 Plaintiffs and the Class in the event of a data breach.

Defendant Fails to Comply with HIPAA Guidelines

100. Essen 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.

101. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[40] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

103. 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.

104. 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.

105. "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.

106. 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.

107. 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).

108. 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.

109. 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***."[41]

110. 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).

111. 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).

112. 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

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

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."[42] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI."[43]

Defendant Fails to Comply with Industry Standards

113. As noted above, experts studying cybersecurity 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.

114. 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; utilizing strong passwords; employing multi-layer security measures, including firewalls, anti-virus and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; and backing up data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including implementation of a multi-factor authentication system.

115. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network

[42] U.S. Department of Health & Human Services, *Security Rule Guidance Material* http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed Mar. 22, 2024).
[43] U.S. Department of Health & Human Services, *Guidance on Risk Analysis* https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed Mar. 22, 2024).

ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failing to train staff.

116. Defendant also 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 established standards in reasonable cybersecurity readiness.

117. 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

118. 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 Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) Plaintiffs' Private Information being disseminated on the

dark web; (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.

The Data Breach Increases Victims' Risk of Identity Theft

119. As Plaintiffs have already experienced, the unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

120. 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 Plaintiffs and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

121. 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.

122. Plaintiffs' and Class Members' Private Information is of great value to hackers and cybercriminals, 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 Plaintiffs and Class Members and to profit off their misfortune.

123. 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.

124. 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."

125. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[44]

126. With "Fullz" packages, cybercriminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

[44] "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 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/.

127. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' telephone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, telephone numbers, or credit card numbers may not be included in the Private Information 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.

128. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

129. Thus, even if certain information (such as insurance information) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package. This comprehensive dossier then can be sold—and 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

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

131. Thus, due to the actual and imminent risk of identity theft, Essen, in its Notice Letter, instructs Plaintiffs and Class Members to take the following measures to protect themselves: "individuals are encouraged to remain vigilant against incidents of identity theft or fraud by reviewing account statements and explanations of benefits and monitoring free credit reports for suspicious activity over the next 12 – 24 months."[45]

132. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing their telephone phone numbers, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

133. Plaintiffs' mitigation efforts are consistent with findings from the U.S. Government Accountability Office (GAO). The GAO 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."[46]

134. Plaintiffs' mitigation efforts are also consistent with the steps that the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity); reviewing credit reports; contacting companies to remove fraudulent charges from accounts; placing a freeze on credit; and correcting credit reports.[47]

---

[45] *Supra* note 2.
[46] *See* U.S. 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. ("GAO Report")
[47] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed Mar. 22, 2024).

135. And for those Class Members who experience actual identity theft and fraud, in its 2007 Report, the GAO noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[48]

Diminution of Value of Private Information

136. PII and PHI are valuable property rights.[49] Their value is axiomatic, considering the value of "Big Data" in corporate America and the consequences of cyberthefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that Private Information has considerable market value.

137. Sensitive PII can sell for as much as $363 per record, according to the Infosec Institute.[50]

138. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[51]

139. In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker, who in turn aggregates the information and provides it to marketers or app developers.[52,53] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[54]

---

[48] *Supra* note 46, at P. 2.
[49] *Id.*
[50] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("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).
[51] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://www.infosecinstitute.com/resources/healthcare-information-security/hackers-selling-healthcare-data-in-the-black-market/.
[52] David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, LA Times, (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[53] DATACOUP, https://datacoup.com/ (last accessed Mar. 22, 2024).
[54] https://digi.me/what-is-digime/

140. 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."[55]

141. According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.[56]

142. As a result of the Data Breach, Plaintiffs' 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 Plaintiffs 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.

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

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

---

[55] EFraudPrevention, *Medical I.D. Theft*, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited Mar. 27, 2024).

[56] 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 Mar. 27, 2024).

145. Plaintiffs 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.

146. Essen was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's networks, amounting to, upon information and belief, thousands of individuals' detailed, sensitive information, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

147. The injuries to Plaintiffs 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 Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

148. Given the type of targeted attack in this case, sophisticated criminal activity, the volume and type of Private Information involved, and Plaintiffs' Private Information already being disseminated on the dark web (as discussed below) 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 victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

149. Such fraud may go undetected until debt collection calls commence months or 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.

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

151. 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 for credit monitoring to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

152. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When submitting Private Information to Defendant for the provision of medical services under certain terms, Plaintiffs and other reasonable patients understood and expected that Defendant would properly safeguard and protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received medical services of a lesser value than what they reasonably expected to receive under the bargains they struck with Essen.

PLAINTIFFS' EXPERIENCES

Plaintiff Marilyn Rivera

153. Plaintiff Rivera is an Essen patient who obtained services there in or about 2021.

154. In order to obtain medical services from Essen, she was required to provide her Private Information to Defendant, including her name, date of birth, Social Security number, and other sensitive information.

155. At the time of the Data Breach—March 14, 2023 through March 22, 2023--Defendant retained Plaintiff Rivera's Private Information in its systems.

156. Plaintiff Rivera 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.

157. Plaintiff received the Notice Letter from Essen, dated December 29, 2023, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties in the Data Breach.

158. As a result of the Data Breach and at the direction of Essen's Notice Letter, which instructs Plaintiff to "remain vigilant against incidents of identity theft or fraud by reviewing account statements and explanations of benefits and monitoring free credit reports for suspicious activity over the next 12 – 24 months[,]"[57] Plaintiff Rivera made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing her phone number, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data 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.

159. 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 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) remains unencrypted and available

[57] *Supra* note 2 (Notice Letter).

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.

160. Plaintiff additionally suffered actual injury in the form of her Private Information being disseminated on the dark web, which, upon information and belief, was caused by the Data Breach.

161. Plaintiff also 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.

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

163. As a result of the Data Breach, Plaintiff Rivera anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Rivera is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

Plaintiff Franchie Muniz

165. Plaintiff Muniz obtained services at Essen as a patient in the past.

166. In order to obtain medical services from Essen, he was required to provide his Private Information to Defendant, including his name, date of birth, Social Security number, and other sensitive information.

167. At the time of the Data Breach—March 14, 2023 through March 22, 2023--Defendant retained Plaintiff Muniz's Private Information in its systems.

168. Plaintiff Muniz is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

169. Plaintiff received the Notice Letter from Essen, in or about January 2024, informing him that his Private Information was improperly accessed and obtained by unauthorized third parties in the Data Breach.

170. As a result of the Data Breach and at the direction of Essen's Notice Letter, which instructs Plaintiff to "remain vigilant against incidents of identity theft or fraud by reviewing account statements and explanations of benefits and monitoring free credit reports for suspicious activity over the next 12 – 24 months[,]"[58] Plaintiff Muniz made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data 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.

171. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time associated

[58] *Id.* (Notice Letter)

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 his 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.

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

173. As a result of the Data Breach, Plaintiff Muniz anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Muniz is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

Plaintiff Michelle Owens

175. Plaintiff Owens obtained services at Essen as a patient in the past.

176. In order to obtain medical services from Essen, she was required to provide her Private Information to Defendant, including her name, date of birth, Social Security number, and other sensitive information.

177. At the time of the Data Breach—March 14, 2023 through March 22, 2023—Defendant retained Plaintiff Owens's Private Information in its systems.

178. Plaintiff Owens 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.

179. Plaintiff received the Notice Letter from Essen, dated December 29, 2023, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties in the Data Breach.

180. As a result of the Data Breach and at the direction of Essen's Notice Letter, which instructs Plaintiff to "remain vigilant against incidents of identity theft or fraud by reviewing account statements and explanations of benefits and monitoring free credit reports for suspicious activity over the next 12 – 24 months[,]"[59] Plaintiff Owens made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching and verifying the legitimacy and impact of the Data Breach; exploring credit monitoring and identity theft insurance options; self-monitoring her accounts with heightened scrutiny; and seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach. Plaintiff has spent significant time dealing with the Data 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.

181. 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

[59] *Id.* (Notice Letter)

Private Information; (iii) lost or diminished value of Private Information; (iv) lost time 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) 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.

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

183. As a result of the Data Breach, Plaintiff Owens anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Owens is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

Plaintiff Florin Carstenoiu

185. Plaintiff Carstenoiu obtained services at Essen as a patient in the past.

186. In order to obtain medical services from Essen, he was required to provide his Private Information to Defendant, including his name, date of birth, Social Security number, and other sensitive information.

187. At the time of the Data Breach—March 14, 2023 through March 22, 2023—Defendant retained Plaintiff Carstenoiu's Private Information in its systems.

188. Plaintiff Carstenoiu is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

189. Plaintiff received the Notice Letter from Essen, in or about January 2024, informing him that his Private Information was improperly accessed and obtained by unauthorized third parties in the Data Breach.

190. As a result of the Data Breach and at the direction of Essen's Notice Letter, which instructs Plaintiff to "remain vigilant against incidents of identity theft or fraud by reviewing account statements and explanations of benefits and monitoring free credit reports for suspicious activity over the next 12 – 24 months[,]"[60] Plaintiff Carstenoiu made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff has spent significant time dealing with the Data 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.

191. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time 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

[60] *Id.* (Notice Letter)

continued and certainly increased risk to his 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.

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

193. As a result of the Data Breach, Plaintiff Carstenoiu anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Carstenoiu is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

Plaintiff Luigi Hernandez

195. Plaintiff Hernandez obtained services at Essen as a patient in the past.

196. In order to obtain medical services from Essen, he was required to provide his Private Information to Defendant, including his name, date of birth, Social Security number, and other sensitive information.

197. At the time of the Data Breach—March 14, 2023 through March 22, 2023—Defendant retained Plaintiff Hernandez's Private Information in its systems.

198. Plaintiff Hernandez is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He

has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

199. Plaintiff received the Notice Letter from Essen, dated December 29, 2023, informing him that his Private Information was improperly accessed and obtained by unauthorized third parties in the Data Breach.

200. As a result of the Data Breach and at the direction of Essen's Notice Letter, which instructs Plaintiff to "remain vigilant against incidents of identity theft or fraud by reviewing account statements and explanations of benefits and monitoring free credit reports for suspicious activity over the next 12 – 24 months[,]"[61] Plaintiff Hernandez made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff has spent significant time dealing with the Data 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.

201. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time 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 his 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.

[61] *Id.* (Notice Letter)

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

203. As a result of the Data Breach, Plaintiff Hernandez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Hernandez is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

Plaintiff Anggie Genao De Hernandez

205. Plaintiff De Hernandez obtained services at Essen as a patient in the past.

206. In order to obtain medical services from Essen, she was required to provide her Private Information to Defendant, including her name, date of birth, Social Security number, and other sensitive information.

207. At the time of the Data Breach—March 14, 2023 through March 22, 2023—Defendant retained Plaintiff De Hernandez's Private Information in its systems.

208. Plaintiff De Hernandez 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.

209. Plaintiff received the Notice Letter from Essen, dated December 29, 2023, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties in the Data Breach.

210. As a result of the Data Breach and at the direction of Essen's Notice Letter, which instructs Plaintiff to "remain vigilant against incidents of identity theft or fraud by reviewing account statements and explanations of benefits and monitoring free credit reports for suspicious activity over the next 12 – 24 months[,]"[62] Plaintiff De Hernandez made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff has spent significant time dealing with the Data 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.

211. 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 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) 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.

[62] *Id.* (Notice Letter)

212. Plaintiff De Hernandez further suffered actual injury in the form of experiencing a fraudulent transaction, for approximately $300, from her Citi Bank checking account, in or about February 2024, which, upon information and belief, was caused by the Data Breach.

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

214. As a result of the Data Breach, Plaintiff De Hernandez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff De Hernandez is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

215. Plaintiff De Hernandez 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 ALLEGATIONS

216. Pursuant to CPLR § 901 *et seq*., Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach announced by Essen in December 2023, including all persons who Essen sent a notice of the Data Breach.

217. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

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

219. Numerosity — CPLR §901(a)(1): The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, thousands of individuals' Private Information was compromised in the Data Breach.

220. Commonality — CPLR §901(a)(2): Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;
b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;
c. Whether Defendant had respective duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;
d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;
e. Whether and when Defendant actually learned of the Data Breach;
f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. 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;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

221. Typicality — CPLR §901(a)(3): Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

222. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

223. Adequacy of Representation — CPLR §901(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

224. Superiority — CPLR §901(a)(5): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

225. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered;

proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

226. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

227. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

228. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

229. Further, 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.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

230. Plaintiffs reallege and incorporate by reference all preceding paragraphs, as if fully set forth herein.

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

232. Essen gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

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

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

235. 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 owed a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

236. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC 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.

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

238. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Essen did not begin to notify Plaintiffs or Class Members of the Data Breach until December 29, 2023 despite, upon information and belief, Defendant knowing shortly after March 17, 2023 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiffs and the Class.

239. Defendant owed duties of care to Plaintiffs 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.

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

241. Defendant's duties 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.

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

243. Defendant also had duties to exercise appropriate clearinghouse practices to remove former patients' Private Information they were no longer required to retain pursuant to regulations.

244. Moreover, Defendant had duties to notify Plaintiffs and the Class promptly and adequately of the Data Breach.

245. Defendant had and continues to have duties to adequately disclose that the Private Information of Plaintiffs 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 Plaintiffs 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.

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

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
b. Failing to adequately monitor the security of its networks and systems;
c. Allowing unauthorized access to Class Members' Private Information;
d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
e. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations,
f. 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; and
g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

247. 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 they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

248. Plaintiffs and Class Members were within the class of persons the FTC Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

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

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

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

252. 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.

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

254. Plaintiffs 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 Plaintiffs 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.

255. 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.

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

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

258. Defendant's duties extended to protecting Plaintiffs 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.

259. Essen has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

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

risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs 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.

262. As a direct and proximate result of Defendant's negligence, Plaintiffs 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 costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) Plaintiffs' Private Information being disseminated on the dark web; (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.

263. As a direct and proximate result of Defendant's negligence, Plaintiffs 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.

264. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs 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.

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

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

267. Plaintiffs 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.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

268. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

270. Plaintiffs and the Class entrusted their Private Information to Defendant. In so doing, Plaintiffs 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 Plaintiffs and the Class if their data had been breached and compromised or stolen.

271. In entering into such implied contracts, Plaintiffs 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.

272. Implicit in the agreement between Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members from unauthorized disclosure or uses; and (f) retain the Private Information only under conditions that kept such information secure and confidential.

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

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

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

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

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

278. Plaintiffs 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.

279. Plaintiffs 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.

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

281. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

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

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

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

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

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

286. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

287. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs' and Class Members' Private Information, Defendant became fiduciaries by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

288. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with its patients, in particular, to keep secure its patients' Private Information.

289. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

290. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

291. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

292. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

293. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs 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) experiencing an increase in spam calls, texts, and/or emails; (vii) Plaintiffs' Private Information being disseminated on the dark web; (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.

294. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Violation of the New York Deceptive Trade Practices Act ("GBL")
New York Gen. Bus. Law § 349
(On Behalf of Plaintiffs and the Class)

295. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

296. 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 Plaintiffs 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 Plaintiffs 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).

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

298. Defendant failed to audit, monitor, and verify the integrity of its networks and data security practices.

299. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security and made affirmative representations regarding its data security commitments and practices.

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

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

302. 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, Plaintiffs 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.

303. Defendant knew or should have known that its 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.

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

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

306. Plaintiffs and Class Members were injured because:

a. Plaintiffs and Class Members would not have obtained services from Defendant had they known the true nature and character of Defendant's data security practices;

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

307. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiffs 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) experiencing an increase

in spam calls, texts, and/or emails; (vii) Plaintiffs' Private Information being disseminated on the dark web; (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.

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

309. Plaintiffs bring this action on behalf of themselves 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 healthcare decisions and to protect Plaintiffs, 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.

310. Plaintiffs and Class Members seek 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.

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

312. Also as a direct result of Defendant's violation of GBL § 349, Plaintiffs and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering 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) immediately provide adequate credit monitoring to all Class Members.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

313. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

314. This claim is pleaded in the alternative to the breach of implied contract and breach of fiduciary duty claims above.

315. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for or had payments made on their behalf for medical services from Essen as well as provided Essen with their Private Information. In exchange, Plaintiffs and Class Members should have received the medical services from Essen that were the subject of the transaction and should have had their Private Information protected with adequate data security.

316. Defendant knew that Plaintiffs and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the Private Information entrusted to them. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

317. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

318. Defendant acquired the Private Information through inequitable record retention as they failed to disclose the inadequate data security practices previously alleged.

319. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted Defendant with their Private Information or obtained medical services at Essen.

320. Plaintiffs and Class Members have no adequate remedy at law.

321. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

322. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: i) 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) experiencing an increase in spam calls, texts, and/or emails; (vii) Plaintiffs' Private Information being disseminated on the dark web; (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.

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs 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 its 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 Plaintiffs and Class Members unless Essen can provide to the Court reasonable justification for the retention and use of such

information when weighed against the privacy interests of Plaintiffs 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 Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs 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 its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's networks are compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. 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 Plaintiffs and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, 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;

xiii. requiring Defendant to implement a system of tests to assess its 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;

xiv. 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;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of its confidential Private

Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified an 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 damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: July 22, 2024

Respectfully submitted,

/s/ Vicki J. Maniatis

Vicki J. Maniatis (NY 2578896)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, NY 11530
Tel: (865) 412-2700
vmaniatis@milberg.com

Gary M. Klinger (*pro hac vice forthcoming*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (270) 821-0656
Fax: (270) 825-1163

Attorneys for Plaintiff Rivera, Index No. 801239/2024E

Andrew W. Ferich (admitted *pro hac vice*)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel: (310) 474-9111
Fax: (310) 474-8585
aferich@ahdootwolfson.com

Tina Wolfson (NY 5436043)
Deborah De Villa (NY 5724315)
AHDOOT & WOLFSON, PC
521 5th Avenue, 17th Floor
New York, NY 10175
Tel: (917) 336-0171
Fax: (917) 336-0177
twolfson@ahdootwolfson.com
ddevilla@ahdootwolfson.com

Attorneys for Plaintiff Carstenoiu, Index No. 801509/2024E

Israel David
Blake Hunter Yagman
ISRAEL DAVID LLC
17 State Street, Suite 4010
New York, NY 10004
Tel: (212) 739-0622
Fax: (212) 739-0628
israel.david@davidllc.com
blake.yagman@davidllc.com

Attorneys for Plaintiff Muniz, Index No. 801574/2024E

Raina C. Borrelli (*pro hac vice forthcoming)*
raina@ straussborrelli.com
STRAUSS BORRELLI PLLC
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423

Eli L. Fuchsberg
JACOB D. FUCHSBERG LAW FIRM
3 Park Ave., Suite 3700
New York, NY 10016
Tel: (212) 869-3500

Attorneys for Hernandez Plaintiffs,
Index No. 801579/2024E

Kevin Laukaitis (*pro hac vice* forthcoming)
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
Tel: (215) 789-4492
klaukaitis@laukaitislaw.com

Attorney for Plaintiff Owens,
Index No. 801222/2024E

Attorney for Plaintiffs and the
Proposed Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 22nd day of July 2024, a true and correct copy of the above and foregoing was filed with the Clerk of Court via the Court's electronic filing system for electronic service on all counsel of record.

The undersigned hereby also certifies that on the 22nd day of July 2024, a true and correct copy of the above and foregoing will be sent via electronic mail to the following:

Daniel M. Braude
dbraude@mullen.law
Claudia D. McCarron
cmccarron@mullen.law
MULLEN COUGHLIN LLC
426 W. Lancaster Ave.
Devon, PA 19333
Telephone: (267) 930-4770

Attorneys for Defendant Essen Medical Associates, P.C.

/s/ Vicki J. Maniatis
Vicki J. Maniatis (NY 2578896)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: (865) 412-2700
vmaniatis@milberg.com