# Exhibit A2

**UNITED STATES DISTRICT COURT**
**DISTRICT OF MARYLAND**
**NORTHERN DIVISION**

| | |
|---|---|
| **EVELYN RIOS,** individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>**MEDSTAR HEALTH INC.**<br><br>Defendant. | Case No.<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Evelyn Rios ("Plaintiff"), on behalf of all others similarly situated, brings this action against Medstar Health Inc. ("MedStar" or "Defendant"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts of public record, and information and belief.

## NATURE OF THE ACTION

1. Plaintiff seeks to hold MedStar responsible for the injuries Medstar inflicted on Plaintiff and hundreds of thousands of similarly situated persons ("Class Members") due to MedStar's impermissibly inadequate and unlawful data security, which caused the personal information of Plaintiff and those similarly situated to be exfiltrated by unauthorized access by cybercriminals (the "Data Breach") between January 25, 2023 and October 18, 2023.

2. MedStar operates as a non profit organization. The Organization offers cancer care, cardiovascular, diabetes, gastroenterology, neurology, mental health, orthopedics, rehabilitation, and urology services. MedStar serves patients in the United States.[1]

3. The Data Breach affected 183,709 individuals.[2] The data which MedStar collected from the Plaintiff and Class Members, and which was exfiltrated by cybercriminals from MedStar, were highly sensitive. The exfiltrated data included personal identifying information ("PII") and personal health information ("PHI" and, together with PII, "Personal Information") such as: name, date of birth, Social Security number, and brokerage and banking information.

4. Upon information and belief, prior to and through the date of the Data Breach, MedStar obtained Plaintiff's and Class Members' Personal Information and then maintained that sensitive data in a negligent and/or reckless manner. As evidenced by the Data Breach, MedStar inadequately and unlawfully maintained its network, platform, software—rendering these easy prey for cybercriminals.

5. Upon information and belief, the risk of the Data Breach was known to MedStar. Thus, MedStar was on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft.

6. Then, after the Data Breach, MedStar failed to provide timely notice to the affected Plaintiff and Class Members, thereby exacerbating their injuries. Ultimately, MedStar deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, MedStar impermissibly left Plaintiff and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

[1] Bloomberg, "MedStar" https://www.bloomberg.com/profile/company/20076Z:US (last visited on May 13, 2024).
[2] U.S. Department of Health and Human Services, Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed May 13, 2024).

7. Even when MedStar finally notified Plaintiff and Class Members of their Personal Information exfiltration, MedStar failed to adequately describe the Data Breach and its effects, as well as the measures it took to prevent data breaches from occurring in the future.

8. Today, the identities of Plaintiff and Class Members are in jeopardy—all because of MedStar's negligence. Plaintiff and Class Members now suffer from a present and continuing risk of fraud and identity theft and must now constantly monitor their financial accounts.

9. Armed with the PII and PHI stolen in the Data Breach, criminals can commit a boundless litany of financial crimes. Specifically, and without limitation, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

10. Plaintiff and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their Personal Information, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

12. Through this action, Plaintiff seeks to remedy these injuries on behalf of themselves and all similarly situated individuals whose Personal Information was exfiltrated and compromised in the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to MedStar's data security systems, future annual audits, and the appointment of an independent and qualified cyber auditor to monitor MedStar's cyber hygiene, all of which will be funded by MedStar.

## PARTIES

14. Plaintiff Rios is a natural person and resident and citizen of Prince George's County, Maryland. Rios is a current client of MedStar. On or about May 3, 2024, Rios received a letter informing her of the Data Breach ("Data Breach Notification"), as described more fully below.

15. Defendant MedStar operates as a non profit organization. The Organization offers cancer care, cardiovascular, diabetes, gastroenterology, neurology, mental health, orthopedics, rehabilitation, and urology services. MedStar serves patients in the United States.[3] MedStar is headquartered in Columbia, MD.

## JURISDICTION AND VENUE

16. This Court has original subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because Plaintiff (and many members of the class) are citizens of states different than that of Defendant MedStar.

[3] Bloomberg, "MedStar" https://www.bloomberg.com/profile/company/20076Z:US (last visited on May 13, 2024).

17. This Court has personal jurisdiction over Defendant MedStar, because MedStar maintains its principal place of business in this district.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and MedStar maintains its principal place of business in the jurisdiction.

## FACTUAL ALLEGATIONS

***Defendant Collected and Stored the Personal Information of Plaintiff and Class Members***

19. Defendant operates a healthcare organization, providing healthcare services throughout the United States.

20. Upon information and belief, MedStar received and maintained the Personal Information of its clients, such as individuals' names, mailing address, dates of birth, date(s) of service, provider name(s), and/or health insurance information. These records were, and continue to be, stored on MedStar's computer systems.

21. Because of the highly sensitive and personal nature of the information MedStar acquires and stores, MedStar knew or reasonably should have known that it stored protected Personal Information and must comply with industry standards related to data security and all federal and state laws protecting customers' Personal Information and provide adequate notice to customers if their Personal Information is disclosed without proper authorization.

22. When MedStar collects this sensitive information, it promises to use reasonable measures to safeguard the Personal Information from theft and misuse.

23. MedStar acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiff's and Class Members' Personal Information.

24. Specifically, MedStar's Privacy Policy states:[4]

> **Our obligation to you**
> MedStar Health is committed to the protection of your medical information. In our mission to serve our patients, it is our vision to be the Trusted Leader in Caring for People and Advancing Health. We create and obtain information about you and use it to provide you with quality care and to comply with certain legal requirements. We are required by law to maintain the privacy of your health information and to give you this Notice of our legal duties, our privacy practices, and your rights. We are required to follow the terms of our most current Notice. When we disclose information to other persons and companies to perform services for us, we will require them to protect your privacy. There are other laws we are required to follow that may provide additional protections, such as laws related to mental health, behavioral health, alcohol and other substance abuse, genetic information, and communicable disease or other health conditions.

25. By obtaining, collecting, receiving, and/or storing Plaintiff's and Class Members' Personal Information, MedStar assumed legal and equitable duties and knew, or should have known, that they were thereafter responsible for protecting Plaintiff's and Class Members' Personal Information from unauthorized disclosure.

26. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Personal Information, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

27. Upon information and belief, Plaintiff and Class Members relied on MedStar to keep their Personal Information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

[4] MedStar, "Patient Privacy Policy," https://www.medstarhealth.org/patient-privacy-policy (last accessed on May 14, 2024).

28. MedStar could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, or better selecting its information technology partners.

29. MedStar's negligence in safeguarding Plaintiff's and Class Members' Personal Information was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

30. Despite the prevalence of public announcements of data breaches and data security compromises, MedStar failed to take appropriate steps to protect Plaintiff's and Class Members' Personal Information from being compromised.

31. MedStar failed to properly select its information security partners.

32. MedStar failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

33. MedStar failed to ensure the proper monitoring and logging of file access and modifications.

34. MedStar failed to ensure the proper training its and its technology partners' employees as to cybersecurity best practices.

35. MedStar failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the Personal Information of Plaintiff and Class Members.

36. MedStar failed to timely and accurately disclose that Plaintiff's and Class Members' Personal Information had been improperly acquired or accessed.

37. MedStar knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured Personal Information.

38. MedStar failed to provide adequate supervision and oversight of the Personal Information with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Personal Information of Plaintiff and Class Members, misuse the Personal Information and potentially disclose it to others without consent.

39. Upon information and belief, MedStar failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

40. Upon information and belief, MedStar failed to ensure the proper encryption of Plaintiff's and Class Members' Personal Information and monitor user behavior and activity to identify possible threats.

***The Data Breach***

41. On or about May 3, 2024, MedStar mailed the Data Breach Notification letter (in the form of Exhibit "A", attached to this Complaint) to its former and current clients, containing, among other the following statements:

> MedStar Health is committed to protecting the privacy and security of the information in our care. We are writing to notify you about a data incident that may have involved some of your information. This letter explains the data incident and the measures we have taken.
>
> **What Happened?**
> We discovered that an outside party had accessed emails and files associated with three MedStar Health employee email accounts. The unauthorized access occurred intermittently between January 25, 2023 and October 18, 2023. On March 6, 2024, after conducting a forensic analysis of the unauthorized access, we determined that your information was included in the emails and files that were accessed. While we

> have no reason to believe that your information was actually acquired or viewed, we cannot rule out such access.
>
> **What Information Was Involved?**
> The emails and files contained information that may have included some or all of the following: your name, mailing address, date of birth, date(s) of service, provider name(s), and/or health insurance information.

42. The Data Breach Notification did not promise any assistance on the part of MedStar, except for a phone line. It did not offer any credit monitoring, identity theft protection or similar measures:

> **What We Are Doing.**
> We take this matter very seriously. We employ appropriate physical, technical, and administrative controls to ensure the safety and confidentiality of your information. Nonetheless, to help prevent something like this from happening again, we have implemented additional safeguards and security measures to enhance our existing controls. We have also notified law enforcement.
>
> **More Information.**
> We remain committed to protecting the confidentiality and security of patient information, and apologize for the concern this may cause. If you have questions, please call us at 1- 888-841-4282, available 9:00 a.m. to 9:00 p.m. Eastern Time.

43. Additionally, MedStar posted the following text on its website:[5]

> On May 3, 2024, we mailed notification letters to certain MedStar Health patients whose personal information may have been involved in a data incident.
>
> We discovered that an outside party had accessed emails and files associated with three MedStar Health employee email accounts. The unauthorized access occurred intermittently between January 25, 2023 and October 18, 2023. On March 6, 2024, after conducting a forensic analysis of the unauthorized access, we determined that patient information was included in the emails and files that were accessed. While we have no reason to believe that patient information was actually acquired or viewed, we cannot rule out such access.
>
> The emails and files contained information that may have included some or all of the following: patients' names, mailing address, dates

[5] MedStar Health, Notice of Data Incident, https://www.medstarhealth.org/notice-of-data-incident (last accessed on May 13, 2024).

> of birth, date(s) of service, provider name(s), and/or health insurance information.
>
> We apologize for any concern or inconvenience this may cause. Patients whose information may have been involved are encouraged to review statements they receive related to their healthcare. If they identify anything unusual related to the healthcare services or the charges for services, they should contact the healthcare entity or health insurer immediately.
>
> We take this matter very seriously. We employ appropriate physical, technical, and administrative controls to ensure the safety and confidentiality of patients' information. Nonetheless, to help prevent something like this from happening again, we have implemented additional safeguards and security measures to enhance our existing controls. We have also notified law enforcement.
>
> We also established a dedicated, toll-free call center to help answer questions about the data incident. The call center can be reached at 1-888-841-4282, available 9:00 a.m. to 9:00 p.m. Eastern Time.

44. It is likely the Data Breach was targeted at the MedStar due to its status as a large healthcare organization that collects, creates, and maintains Personal Information, as well as creating and maintaining entities for wealthy clients.

45. MedStar was untimely and unreasonably delayed in providing notice of the Data Breach to Plaintiff and Class Members.

46. Time is of the essence when highly sensitive Personal Information is subject to unauthorized access and/or acquisition.

47. The disclosed, accessed, and/or acquired Personal Information of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Personal Information to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Personal Information onto the Dark Web. Plaintiff and Class Members

now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

48. In sum, MedStar largely put the burden on Plaintiff and Class Members to take measures to protect themselves.

49. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[6]

50. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[7] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[8] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

---

[6] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=%20In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed April 25, 2024); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data, https://www.bls.gov/news.release/pdf/wkyeng.pdf* (last accessed April 25, 2024) (finding that on average, private-sector workers make $1,145 per 40-hour work week.).

[7] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019) (last accessed April 25, 2024).

[8] *Id.*

51. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

52. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' Personal Information with the intent of engaging in misuse of the Personal Information, including marketing and selling Plaintiff's and Class Members' Personal Information.

53. MedStar has offered no measures to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide Plaintiff and Class Members identity theft protection services for 10 years.

54. Defendant had and continues to have obligations created by reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' Personal Information confidential and to protect such Personal Information from unauthorized access.

55. Plaintiff and the Class Members remain, even today, in the dark regarding the scope of the data breach, what particular data was stolen, beyond several categories listed in the letter as "included" in the Data Breach, and what steps are being taken, if any, to secure their Personal Information and financial information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly the Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

56. Plaintiff's and Class Members' Personal Information and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Personal Information and financial information for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the Personal Information and/or financial information of Plaintiff and Class Members.

***Defendant Failed to Comply with FTC Guidelines***

57. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[9] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exfiltration of Personal Information.

58. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[10] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

59. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

---

[9] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed April 25, 2024).

[10] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed April 25, 2024).

60. The FTC recommends that companies not maintain Personal 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.[11]

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

62. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

***Defendant Failed to Follow Industry Standards***

63. Despite its alleged commitments to securing sensitive data, MedStar does not follow industry standard practices in securing Personal Information.

64. Experts studying cyber security routinely identify financial service providers as being particularly vulnerable to cyberattacks because of the value of the Personal Information which they collect and maintain.

65. Several best practices have been identified that at a minimum should be

[11] *See Start With Security, A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 16, 2024).

implemented by financial service providers like MedStar, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

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

67. MedStar failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

68. Such frameworks are the existing and applicable industry standards in the financial service industry. MedStar failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

***The Experiences and Injuries of Plaintiff and Class Members***

69. Plaintiff and Class Members are current and former clients of MedStar.

70. As a prerequisite of obtaining medical services from MedStar, MedStar required its clients —like Plaintiff and Class Members—to disclose their Personal Information.

71. Following the Data Breach, Plaintiff Rios noticed several inquiries on her credit report. Criminals attempted to obtain a loan, a credit card and to purchase a car in her name. Further, when Plaintiff attempted to consolidate her student loan, she was initially denied the opportunity to do so due to these fraudulent transaction attempts, resulting from the Data Breach, which generated "hard inquiries" on her credit record.

72. Plaintiff had to place multiple calls to the relevant companies to minimize the impact of these fraudulent transaction attempts, resulting from the Data Breach, on her credit rating. She spent in excess of 15 hours addressing these fraudulent transactions.

73. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided Defendant with her Personal Information had MedStar disclosed that it lacked security practices adequate to safeguard PII and PHI.

74. Plaintiff suffered actual injury in the form of damages and diminution in the value of her Personal Information – a form of intangible property that she entrusted to MedStar.

75. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increase concerns for the loss of her privacy, especially her PHI.

76. Plaintiff reasonably believes that her Personal Information may have already been sold to by the cybercriminals. Had she been notified of MedStar's Data Breach in a more timely manner, she could have attempted to mitigate her injuries.

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

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

79. When MedStar finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Defendant's Breach Notice fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Data Breach was perpetrated by, and the extent to which those data elements were compromised.

80. Because of the Data Breach, MedStar inflicted injuries upon Plaintiff and Class Members. And yet, MedStar has done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

81. All Class Members were injured when MedStar caused their Personal Information to be exfiltrated by cybercriminals.

82. Plaintiff and Class Members entrusted their Personal Information to MedStar. Thus, Plaintiff had the reasonable expectation and understanding that MedStar would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. Plaintiff and Class Members would not have entrusted their Personal Information to MedStar had they known that Defendant would not take reasonable steps to safeguard their information.

83. Plaintiff and Class Members suffered actual injury from having their Personal Information compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their Personal Information—a form of property that MedStar obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their Personal Information;

(d) fraudulent activity resulting from the Data Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

84. As a result of the Data Breach, Plaintiff and Class Members also suffered emotional distress because of the release of their Personal Information—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiff and Class Members suffer from anxiety about unauthorized parties viewing, selling, and/or using their Personal Information for nefarious purposes like identity theft and fraud.

85. Plaintiff and Class Members also suffer anxiety about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions.

86. Because of the Data Breach, Plaintiff and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

***Plaintiff and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft***

87. Plaintiff and Class Members suffered injury from the misuse of their Personal Information that can be directly traced to MedStar.

88. The ramifications of MedStar's failure to keep Plaintiff's and the Class's Personal Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

89. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[12]

90. As a result of MedStar's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their Personal Information;

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

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Personal Information; and

[12] Anne Saita, "Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims", Threat Post, (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited on May 14, 2024).

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

91. Stolen Personal Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Personal Information can be worth up to $1,000.00 depending on the type of information obtained.[13]

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

93. It can take victims years to spot or identify Personal Information theft, giving criminals plenty of time to milk that information for cash.

94. One such example of criminals using Personal Information for profit is the development of "Fullz" packages.[14]

[13] Brian Stack, "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/ (last visited on May 14, 2024).

[14] "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 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/tag/fullz/ (last visited on May 14, 2024).

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

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

97. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

98. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their Personal Information had been stolen.

99. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

100. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their Personal Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

101. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Personal Information. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

102. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[15]

***Defendant Failed to Comply with FTC Guidelines***

103. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[16] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed;

[15] "Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable," FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on May 14, 2024).
[16] "Start With Security, A Guide for Business," FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 14, 2024).

(4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[17]

104. According to the FTC, unauthorized Personal Information disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[18] The FTC treats 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(a) of the FTC Act (the "FTCA").

105. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. See *In the matter of Lookout Services, Inc.*, No. C-4326, Complaint ¶ 7 (June 15, 2011) ("[Respondent] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Respondent] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave &*

[17] *Id.*

[18] "Taking Charge, What to Do If Your Identity is Stolen," U.S. DEPARTMENT OF JUSTICE, at 3 (January 2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited on May 14, 2024).

*Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Respondent] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . .").

106. These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of Personal Information.

***Defendant Failed to Comply with HIPAA***

107. Because of its involvement with electronic personal health information ("PHI"), Defendant is a "Business Associate" as defined under the rules and regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (45 CFR Parts 160 to 164). The HIPAA "Security Rule," published in 2003, addresses the requirement that both Covered Entities and Business Associates, as defined therein, adopt security procedures to assure the confidentiality, integrity, and availability of personal health care information, or PHI (45 CFR Part 160 and Subparts A and C of Part 164).[19]

108. Business Associates are directly liable for violations of the HIPAA Security Rule (See HITECH Act 13401, 42 U.S.C. 17931 (making 45 CFR 164.308, 164.310, 164.312, and 164.316 directly applicable to business associates, as well as any other security provision that the HITECH Act made applicable to covered entities); 45 CFR 164.306, 164.308, 164.310, 164.312, 164.314, 164.316.

109. Data Breach is a Security Incident under HIPAA because it impaired both the

[19] The Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited April 30, 2024).

integrity (data is not interpretable) and availability (data is not accessible) of PHI held by MedStar:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[20]

110. The Data Breach is also considered a breach under the HIPAA Rules because there was an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.402.[21]

111. The Security Incident Procedures standard at 45 C.F.R. § 164.308(a)(6)(i) requires a covered entity to implement policies and procedures to address security incidents. The associated implementation specification for response and reporting at § 164.308(a)(6)(ii) requires a covered entity to identify and respond to suspected or known security incidents, mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, and document security incidents and their outcomes.

112. MedStar failed to comply with HIPAA, both prior to and after suffering the Data Breach.

113. Charged with handling highly sensitive Personal Information including, financial information, and health and medical insurance information, MedStar knew or should have known the importance of safeguarding the Personal Information that was entrusted to it. MedStar also knew or should have known of the foreseeable consequences if its data security systems were

[20] FACT SHEET: Ransomware and HIPAA, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last visited May 14, 2024).
[21] *Id.*

breached. This includes the significant costs that would be imposed on MedStar's customers as a result of a breach. MedStar nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

114. MedStar's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the Personal Information of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

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

## CLASS ACTION ALLEGATIONS

116. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

117. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons residing in the United States whose Personal Information was impacted by the Data Breach at MedStar and its affiliated entities, which occurred on or about January 25, 2023 to October 18, 2023.

118. The Class defined above is readily ascertainable from information in MedStar's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

119. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and these entities' current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

120. Plaintiff reserves the right to amend or modify the Class definition—including potential Subclasses—as this case progresses.

121. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

122. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of hundreds of thousands of individuals who reside in the U.S. and were or are clients of MedStar, and whose Personal Information was compromised by the Data Breach.

123. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If MedStar unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personal Information;

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

c. If MedStar's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. If MedStar's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If MedStar owed a duty to Class Members to safeguard their Personal Information;

f. If MedStar breached its duty to Class Members to safeguard their Personal Information;

g. If MedStar failed to comply with the HIPAA Security Rule (45 CFR 160 and Subparts A and C of Part 164) by failing to implement reasonable security procedures and practices to protect the integrity and availability of PHI;

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

i. If MedStar should have discovered the Data Breach earlier;

j. If MedStar took reasonable measures to determine the extent of the Data Breach after it was discovered;

k. If MedStar failed to provide notice of the Data Breach in a timely manner;

l. If MedStar's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

m. If MedStar's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

n. If MedStar's conduct was negligent;

o. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

p. If Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

q. If MedStar breached implied contracts with Plaintiff and Class Members;

r. If MedStar was unjustly enriched as a result of the Data Breach; and

s. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

124. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, all Plaintiff and Class Members were subjected to Defendant's uniformly illegal and impermissible conduct.

125. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

126. **Predominance**. MedStar has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the

same network system and unlawfully and inadequately protected in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

127. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

128. The litigation of the claims brought herein is manageable. MedStar'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.

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

130. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above, including in paragraph 112.

131. MedStar 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.

## FIRST CAUSE OF ACTION
### Negligence
### (On Behalf of Plaintiff and the Class)

132. Plaintiff re-alleges and incorporate by reference paragraphs 1-131 of the Complaint as if fully set forth herein.

133. MedStar required its employees and contractors to submit Plaintiff's and Class Members' non-public Personal Information to MedStar to receive MedStar's services.

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

135. The risk that unauthorized persons would attempt to gain access to the Personal Information and misuse it was foreseeable to MedStar. Given that MedStar holds vast amounts of Personal Information, it was inevitable that unauthorized individuals would at some point try to access MedStar's databases of Personal Information.

136. After all, Personal Information is highly valuable, and MedStar knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiff and Class Members. Thus, MedStar knew, or should have known, the importance of exercising reasonable care in handling the Personal Information entrusted to them.

137. MedStar owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its, or its service providers', systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

138. MedStar's duty of care to use reasonable security measures arose because of the special relationship that existed between MedStar and Plaintiff and Class Members, which is recognized by laws and regulations, as well as common law. MedStar was in a superior position to ensure that its own, and its service providers', systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

139. MedStar failed to take appropriate measures to protect the Personal Information of Plaintiff and the Class. MedStar is morally culpable, given the prominence of security breaches in the financial services industry, including the insurance industry. Any purported safeguards that MedStar had in place were wholly inadequate.

140. MedStar breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Personal Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the financial service industry, and allowing unauthorized access to Plaintiff's and the other Class Members' Personal Information.

141. The MedStar was negligent in failing to comply with industry and federal regulations in respect of safeguarding and protecting Plaintiff's and Class Members' Personal Information.

142. But for MedStar's wrongful and negligent breach of its duties to Plaintiff and the Class, Plaintiff's and Class Members' Personal Information would not have been compromised, stolen, and viewed by unauthorized persons. MedStar's negligence was a direct and legal cause of the theft of the Personal Information of Plaintiff and the Class and all resulting damages.

143. MedStar owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to its Personal Information. MedStar also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members to take appropriate measures to protect its Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of the Data Breach.

144. MedStar owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals who MedStar knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, MedStar actively sought and obtained the Personal Information of Plaintiff and Class Members.

145. MedStar breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Personal Information. The specific negligent acts and omissions committed by MedStar include, but are not limited to:

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

b. Failing to comply with—and thus violating—FTCA, HIPAA and the applicable regulations;

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

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

e. Allowing unauthorized access to Class Members' Personal Information;

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

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

146. It was foreseeable that MedStar's failure to use reasonable measures to protect Class Members' Personal Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial service industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' Personal Information would result in one or more types of injuries to Class Members.

147. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of MedStar's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' Personal Information. MedStar knew or should have known that its systems and technologies for processing and securing the Personal Information of Plaintiff and the Class had security vulnerabilities.

148. As a result of MedStar's negligence, the Personal Information and other sensitive information of Plaintiff and Class Members was compromised, placing them at a greater risk of

identity theft and their Personal Information being disclosed to third parties without the consent of Plaintiff and the Class Members.

149. Simply put, MedStar's negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their Personal Information by criminals, improper disclosure of their Personal Information, lost benefit of their bargain, lost value of their Personal Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by MedStar's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

150. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

151. Plaintiff and Class Members are also entitled to injunctive relief requiring MedStar to, *e.g.,* (1) strengthen its data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for a period of ten years.

**SECOND CAUSE OF ACTION**
**Negligence *Per Se***
**(On Behalf of Plaintiff and the Class)**

152. Plaintiff re-alleges and incorporates by reference paragraphs 1-131 of the Complaint as if fully set forth herein.

153. Under the Federal Trade Commission Act, MedStar had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of .[22]

[22] 15 U.S.C. § 45.

154. Moreover, Plaintiff's and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that MedStar inflicted upon Plaintiff and Class Members.

155. MedStar's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because MedStar is bound by industry standards to protect confidential Personal Information.

156. MedStar violated its duties and its obligations under HIPAA as a Business Associate by reason of the Data Breach.

**THIRD CAUSE OF ACTION**
**Breach of Contract**
**(On Behalf of the Plaintiff and the Class)**

157. Plaintiff re-alleges and incorporate by reference paragraphs 1-131 of the Complaint as if fully set forth herein.

158. Plaintiff and Class Members entered into a valid and enforceable contract through which they paid money to Defendant in exchange for services. That contract included promises by MedStar to secure, safeguard, and not disclose Plaintiff's and Class Members' Personal Information.

159. Plaintiff and Class Members fully performed their obligations under their contracts with MedStar.

160. However, MedStar did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Personal Information, and therefore MedStar breached its contracts with Plaintiff and Class Members.

161. MedStar allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class Members' Personal Information without permission. Therefore, MedStar breached its contract with Plaintiff and Class Members.

162. MedStar's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in MedStar providing services to Plaintiff and Class Members that were of a diminished value.

163. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including in MedStar's failure to fully perform its part of the bargain with Plaintiff and Class Members.

164. As a direct and proximate result of MedStar's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

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

166. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring MedStar to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiff and Class Members for a period of ten years.

## FOURTH CAUSE OF ACTION
**Breach of Implied Contract**
**(On Behalf of the Plaintiff and the Class)**

167. Plaintiff re-alleges and incorporates by reference paragraphs 1-131 of the Complaint as if fully set forth herein.

168. This claim is pleaded in the alternative to the Third Cause of Action, above.

169. Plaintiff and Class Members were required to deliver their Personal Information to MedStar as part of the process of obtaining financial services from Defendant.

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

171. MedStar accepted possession of Plaintiff's and Class Members' Personal Information, for the ostensible purpose of contracting with Plaintiff and Class Members.

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

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

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

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

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

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

178. Plaintiff and Class Members would not have entrusted their Personal Information to MedStar in the absence of its implied promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

179. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with MedStar. MedStar, on the other hand, breached its obligations under the implied contracts with Plaintiff and Class Members by failing to safeguard their Personal Information and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

180. As a direct and proximate result of MedStar's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Personal Information; (iii) lost or diminished value of Personal Information; (iv) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly

increased risk to their Personal Information, which (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in MedStar's possession and is subject to further unauthorized disclosures so long as MedStar's fails to undertake appropriate and adequate measures to protect the Personal Information.

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

182. Plaintiff and Class Members are also entitled to injunctive relief requiring MedStar to, *e.g.,* (1) strengthen its data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for a period of ten years.

**FIFTH CAUSE OF ACTION**
**Unjust Enrichment**
**(On Behalf of the Plaintiff and the Class)**

183. Plaintiff re-alleges and incorporates by reference paragraphs 1-131 of the Complaint as if fully set forth herein.

184. This Claim is pleaded in the alternative to Third and Fourth Causes of Action, above.

185. Upon information and belief, MedStar funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

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

187. Plaintiff and Class Members conferred a monetary benefit on MedStar. Specifically, they purchased goods and services from MedStar and/or its agents and in so doing

provided MedStar with their Personal Information. In exchange, Plaintiff and Class Members should have received from MedStar the goods and services that were the subject of the transaction and have their Personal Information protected with adequate data security.

188. MedStar knew that Plaintiff and Class Members conferred a benefit which MedStar accepted. MedStar profited from these transactions and used the Personal Information of Plaintiff and Class Members for business purposes.

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

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

191. MedStar failed to secure Plaintiff's and Class Members' Personal Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

192. MedStar acquired the Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

193. If Plaintiff and Class Members knew that MedStar had not reasonably secured their Personal Information, they would not have agreed to provide their Personal Information to MedStar.

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

195. As a direct and proximate result of MedStar's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Personal Information is used; (c) the compromise, publication, and/or theft of their Personal Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Personal Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Personal Information, which remains in MedStar's possession and is subject to further unauthorized disclosures so long as MedStar fails to undertake appropriate and adequate measures to protect Personal Information in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

197. MedStar should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In

the alternative, MedStar should be compelled to refund the amounts that Plaintiff and Class Members overpaid for MedStar's services.

**SIXTH CAUSE OF ACTION**
**Invasion of Privacy**
**(On Behalf of Plaintiff and Class Members)**

198. Plaintiff re-alleges and incorporates by reference paragraphs 1-131 of the Complaint as if fully set forth herein.

199. Plaintiff and Class Members had a legitimate expectation of privacy in their Personal Information, and were entitled to the protection of this information against disclosure to unauthorized third parties.

200. MedStar owed a duty to Plaintiff and Class Members to keep their Personal Information confidential.

201. MedStar failed to protect such information, and permitted unknown third parties to exfiltrate Plaintiff's and Class Members' Personal Information.

202. The unauthorized access to, and exfiltration of, Plaintiff and Class Members' Personal Information is highly offensive to a reasonable person.

203. The Data Breach constituted an intrusion into a place or thing, which is private, and is entitled to be private. Plaintiff and Class Members disclosed their Personal Information to MedStar as part of their use of MedStar's medical services, but privately, with the intention that Personal Information be kept confidential and be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

204. The Data Breach at the hands of the MedStar constitutes an intentional interference with the Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons

or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

205. MedStar acted with a knowing state of mind when it permitted the Data Breach because it had actual knowledge that its information security practices were inadequate and insufficient.

206. As a proximate result of the above acts and omissions of MedStar, the Personal Information of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

207. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

208. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

## PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representatives, and the undersigned as Class Counsel;

B. A mandatory injunction directing MedStar to adequately safeguard the Personal Information of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting MedStar from engaging in the wrongful and unlawful acts

described herein;

ii. requiring MedStar to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring MedStar to delete and purge the Personal Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring MedStar to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Personal Information;

v. requiring MedStar to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on MedStar's systems on a periodic basis;

vi. prohibiting MedStar from maintaining Plaintiff's and Class Members' Personal Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring MedStar to segment data by creating firewalls and access controls so that, if one area of MedStar's network is compromised, hackers cannot gain access to other portions of MedStar's systems;

viii. requiring MedStar to conduct regular database scanning and securing checks;

ix. requiring MedStar to monitor ingress and egress of all network traffic;

x. requiring MedStar 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 Information, as well as protecting the Personal Information of Plaintiff and Class Members;

xi. requiring MedStar 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 MedStar's policies, programs, and systems for protecting personal identifying information;

xii. requiring MedStar to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor MedStar's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

xiii. appointing an independent and qualified cyber auditor to monitor MedStar's cyber hygiene, to be funded by MedStar; and

xiv. requiring MedStar to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that MedStar provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Personal Information to unauthorized persons;

D. A mandatory injunction requiring MedStar to purchase credit monitoring and identity theft protection services for each Class Member for ten years;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

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

**JURY TRIAL DEMANDED**

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: May 15, 2024

Respectfully Submitted,

*/s/ Hassan Zavareei*


| | |
|---|---|
| John A. Yanchunis*<br>Florida Bar #: 324681<br>JYanchunis@forthepeople.com<br>Ronald Podolny*<br>ronald.podolny@forthepeople.com<br>**MORGAN & MORGAN** | Hassan A. Zavareei<br>Attorney ID: 0207150001<br>hzavareei@tzlegal.com<br><br>**TYCKO & ZAVAREEI LLP** |

| | |
|---|---|
| **COMPLEX LITIGATION GROUP**<br>201 North Franklin Street 7th Floor<br>Tampa, FL 33602<br>T: (813) 223-5505<br>F: (813) 223-5402 | 2000 Pennsylvania Ave. NW - Suite 1010<br>Washington, D.C. 20006<br>T: (202) 973-0910 |


**Pro hac vice forthcoming*

***Counsel for Plaintiff and the Class***