Exhibit A4

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MARYLAND
NORTHERN DIVISION

TRACY SANDERS, individually and on behalf of all others similarly situated,

Contact through attorneys: Mason LLP, 5335 Wisconsin Ave. NW, Ste. 640, Washington, DC 20015

County of Residence: Harford County, MD

Plaintiff(s),

v.

MEDSTAR HEALTH, INC,

Address: 10980 Grantchester Way, 6th Floor, Columbia, MD 21044

County of Residence: Howard County, MD

Defendant.

CASE NO.: _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

1. Plaintiff(s) Tracy Sanders ("Plaintiff(s)"), individually and on behalf of all others similarly situated, bring this action against Defendant MedStar Health, Inc. ("MedStar" or "Defendant") to obtain damages, restitution, and injunctive relief from Defendant. Plaintiff(s) make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

2. This class action arises out of Defendant MedStar's failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiff(s)' and Class Members' sensitive personal identifiable information that it had acquired and stored for its business purposes. This failure to secure and monitor its network resulted in 10-month long data breach ("Data Breach") of highly sensitive documents and information stored on the computer network of MedStar, an organization that provides medical treatment and/or employment to individuals, including Plaintiff(s) and Class Members.

3. Defendant's data security failures allowed a targeted cyberattack beginning around January 2023 to compromise Defendant's network (the "Data Breach") that contained personally identifiable information ("PII") and protected health information ("PHI") (collectively, "the Private Information") of Plaintiffs and other individuals ("the Class").

4. According to a notice MedStar sent to the Department of Health and Human Services Office for Civil Rights ("HHS") on or about May 3, 2024, about 183,079 people have been affected.[1]

5. According to a notice on its website, Defendant confirmed that a "data incident" occurred on its network between January 25, 2023 and October 18, 2023.

6. Defendant's website notice states: "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."[2]

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed May 10, 2024).
[2] https://www.medstarhealth.org/notice-of-data-incident (last accessed May 10, 2024).

7. Despite learning of the Data Breach in or about October 2023, and determining that Private Information was involved in the breach beginning on January 25, 2023, Defendant did not begin sending notices of the Data Breach (the "Notice of Data Breach Letter") until May 3, 2024.

8. The Private Information compromised in the Data Breach included certain personal or protected health information of current and former employees and patients, including Plaintiff(s). This Private Information included, but is not limited to: patients' names, mailing address, dates of birth, date(s) of service, provider name(s), and/or health insurance information.[3]

9. The Private Information compromised in what MedStar refers to as a "data incident" in which it "discovered that an outside party had accessed emails and files associated with three MedStar Health employee email accounts."[4] In other words, the cybercriminals intentionally targeted MedStar for the highly sensitive Private Information it stores on its computer network, attacked the insufficiently secured network, then exfiltrated highly sensitive PII and PHI, including but not limited to Social Security numbers. As a result, the Private Information of Plaintiff(s) and Class remains in the hands of those cyber-criminals.

10. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for either treatment or employment or both.

11. Plaintiff(s) bring this class action lawsuit on behalf of themselves and all others similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff(s) and other Class Members that their information had been subject to the unauthorized

[3] *Id.*
[4] *See* Plaintiff Notice Letter, attached as Exhibit A.

access of an unknown third party and including in that notice precisely what specific types of information were accessed and taken by cybercriminals.

12. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant MedStar's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff(s)' 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.

13. Defendant disregarded the rights of Plaintiff(s) and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff(s)' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class Members with prompt and full notice of the Data Breach.

14. In addition, Defendant MedStar failed to properly monitor the computer network and systems that housed the Private Information. Had MedStar properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals almost a month of unimpeded access to the PII and PHI of Plaintiff(s) Class Members.

15. Plaintiff(s)' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant MedStar collected and maintained is now in the hands of data thieves.

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

17. As a result of the Data Breach, Plaintiff(s) and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff(s) and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft.

18. Plaintiff(s) and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

19. Through this Complaint, Plaintiff(s) seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

20. Accordingly, Plaintiff(s) brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, (iv) breach of fiduciary duty; and (v) unjust enrichment, and (vi) declaratory relief.

21. Plaintiff(s) seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to

Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

PARTIES

22. Plaintiff Tracy Sanders is and at all times mentioned herein was an individual citizen of the State of Maryland, residing in the city of Forest Hill, and was a patient of MedStar. Plaintiff Sanders received notice of the Data Breach dated May 3, 2024, attached in Exhibit A.

23. MedStar Health, Inc. is a Maryland non-stock corporation that has its principal place of business at 10980 Grantchester Way, 6th floor, Columbia, Maryland 21044. It can be served through its registered agent, The Corporation Trust, at 2405 York Road, Suite 201, Lutherville Timonium, Maryland 21093.

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

25. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State as a corporation; it maintains its headquarters in Maryland; and committed tortious acts in Maryland.

26. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which MedStar Healthcare is headquartered and has the most significant contacts.

FACTUAL ALLEGATIONS

Defendant's Business

27. Defendant MedsStar is "the largest healthcare provider in Maryland and the Washington, D.C., region."[5]

28. The MedStar system includes "more than 300 care locations include 10 hospitals, 33 urgent care clinics, ambulatory care centers, and primary and specialty care providers. [It is] also home to the MedStar Health Research Institute and a comprehensive scope of health-related organizations."[6]

29. MedStar has more that 33,000 employees, including "physicians, nurses, and many other clinical and non-clinical associates."[7]

30. MedStar offers a wide range of services including primary care, urology, behavioral health, bariatrics, sports medicine, women's care, dermatology, and much more.[8]

31. MedStar has more than 300 healthcare locations in Maryland, Virginia, and Washington DC.[9]

32. For the purposes of this Class Action Complaint, all of MedStar's associated locations will be referred to collectively as "MedStar."

33. In the ordinary course of receiving medical care services from Defendant MedStar, or alternatively being employed by MedStar, each patient and employee must provide (and Plaintiff(s) did provide) Defendant MedStar with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;

[5]https://www.medstarhealth.org/about/facts-and-figures (last accessed May 10, 2024).
[6] *Id.*
[7] *Id.*
[8] https://www.medstarhealth.org/services (last accessed May 10, 2024).
[9] https://www.medstarhealth.org/ (last accessed May 10, 2024).

- Date of birth;
- Social Security number;
- Marital status;
- Employer with contact information;
- Primary and secondary insurance policy holders' name, address, date of birth, and Social Security number;
- Demographic information;
- Driver's license or state or federal identification;
- Information relating to the individual's medical and medical history;
- Insurance information and coverage; and
- Banking and/or credit card information.

34. Defendant also creates and stores medical records and other protected health information for its patients, records of treatments and diagnoses.

35. Upon information and belief, MedStar's HIPAA Notice of Privacy Practices ("Privacy Policy") is provided to every patient both prior to receiving treatment and upon request.[10] MedStar's Privacy Notice makes clear that it understands that its patients' Private Information is personal and must be protected by law.

36. Defendant MedStar agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiff(s) and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

[10] https://www.medstarhealth.org/patient-privacy-policy (last accessed May 10, 2024).

37. Yet, through its failure to properly secure the Private Information of Plaintiff(s) and Class, MedStar failed to meet its own promises of patient privacy.

38. The patient information held by Defendant MedStar in its computer system and network included the highly sensitive Private Information of Plaintiff(s) and Class Members.

The Data Breach

39. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like MedStar.

40. According to Defendant's website Notice, it is unclear of when it learned of a cyber-attack on its computer systems which occurred over a course of 10 months beginning in January 2023, when it intermittently took many of the healthcare provider's networked systems offline, adversely affecting patient treatment, scheduling, and the ability to access patient histories.[11]

41. Defendant notified HHS of the Data Breach on or about May 3, 2024, listing only 183,079 people affected.

42. In January 2023, HHS created a presentation specifically for healthcare providers and IT departments, warning entities like MedStar of the severe threats posed by Royal, BlackCat and similar cybercriminal groups.[12] Within the healthcare industry, the risk of a cyber attack is well-known and preventable with adequate security systems in place.

43. On or about May 3, 2024, months after MedStar learned that the Class's Private Information was attacked by cybercriminals, MedStar patients began receiving their notices of the Data Breach informing them that its investigation determined that their Private Information was accessed.

[11] https://www.medstarhealth.org/notice-of-data-incident (last accessed May 10, 2024).
[12] https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf (last accessed May 10, 2024).

44. MedStar's notice letters list, time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. It failed to provide even one year of credit monitoring that Plaintiffs and Class Members would have to affirmatively sign up for and a call center number that victims may contact with questions, MedStar offered no other substantive steps to help victims like Plaintiff(s) and Class Members to protect themselves. On information and belief, MedStar sent a similar generic letter to all other individuals affected by the Data Breach.

45. MedStar's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

46. MedStar knew or should have known that its electronic records would be targeted by cybercriminals.

47. MedStar had obligations created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiff(s) and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

The Data Breach was a
Foreseeable Risk of which Defendant was on Notice.

49. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including MedStar, are well-aware of the risk of being targeted by cybercriminals.

50. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

51. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss." [13]

52. Individuals, like Plaintiff(s) and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

53. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff(s) and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

54. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state

[13] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed May 10, 2024).

motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[14]

55. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[15]

56. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[16]

57. Cyberattacks 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, and hopefully can ward off a cyberattack.

58. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [17] This publication also explains that "[t]he FBI does

[14] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed May 10, 2024).
[15] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed May 10, 2024).
[16] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed May 10, 2024).
[17] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed May 10, 2024).

not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[18]

59. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, MedStar failed to take appropriate steps to protect the PII of Plaintiff(s) and the proposed Class from being compromised.

Data Breaches are Rampant in Healthcare.

60. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

61. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[19]

62. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health

[18] *Id.*
[19] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last accessed May 10, 2024).

insurance information, and medical and clinical data, and that information can be easily monetized."[20]

63. The HIPAA Journal article goes on to explain that patient records, like those stolen from MedStar, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[21]

64. Data breaches such as the one experienced by Defendant MedStar have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

65. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[22]

66. HHS data shows more than 39 million patients' information was exposed in the first half of 2023 in nearly 300 incidents and that healthcare beaches have doubled between 2020 and 2023, according to records compiled from HHS data by Health IT Security.[23]

67. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In

---

[20] *Id.*
[21] *Id.*
[22] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last accessed May 10, 2024).
[23] https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far (last accessed May 10, 2024).

fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[24]

68. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant MedStar.

Defendant Fails to Comply with FTC Guidelines.

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

70. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[25] 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.[26]

---

[24] https://www.ahu.edu/blog/data-security-in-healthcare (last accessed May 10, 2024).
[25] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 10, 2024).
[26] *Id*.

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

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

73. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

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

75. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

76. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards.

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

78. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

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

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

81. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to and failing to thwart the Data Breach.

Defendant's Conduct Violates HIPAA.

82. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information (PHI).

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

84. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

85. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

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

Defendant has Breached its Obligations to Plaintiff(s) and Class.

87. Defendant breached its obligations to Plaintiff(s) and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer

systems and its patients' data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

88. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff(s)' and Class Members' Private Information.

89. Accordingly, as outlined below, Plaintiff(s) and Class Members now face an increased risk of fraud and identity theft.

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft.

90. Data Breaches such as the one experienced by Plaintiff(s) and the Class are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

91. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[27] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff(s) and Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

92. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report"). [28]

93. The FTC, like the GAO (*see* Exhibit B), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting

[27] https://www.gao.gov/assets/gao-19-230.pdf (last accessed May 10, 2024).*See* attached as Ex. B.

[28] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed May 10, 2024). ("2007 GAO Report").

companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[29]

94. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

95. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

96. Theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[30]

97. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:

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

See 2007 GAO Report, at p. 29.

[29] *See* https://www.identitytheft.gov/Steps (last accessed May 10, 2024).
[30] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

98. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

99. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff(s) and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff(s) and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

100. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[31]

101. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[32] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[33] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's

[31] https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last accessed May 10, 2024).
[32] *Identity Theft and Your Social Security Number*, Social Security Administration (last accessed March 16, 2023). (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed March 16, 2023).
[33] *Id.* at 4.

employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

102. Moreover, it is not an 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. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[34]

103. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[35]

104. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF(S)' EXPERIENCES

Plaintiff Tracy Sanders

[34] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed May 10, 2024).

[35] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed May 10, 2024).

105. Plaintiff Tracy Sanders is and at all times mentioned herein was an individual citizen residing in the State of Maryland.

106. Plaintiff Sanders is and was a patient of MedStar at all times relevant to this Complaint. Plaintiff Sanders received a Notice of Data Breach Letter, related to MedStar's Data Breach dated May 3, 2024. *See* Exhibit A.

107. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her "name, mailing address, date of birth, date(s) of service, provider name(s), and/or health insurance information." *See* Ex. A.

108. Plaintiff Sanders is especially alarmed by the vagueness of her stolen extremely private medical information (PHI) and equally by the fact that her Social Security number was identified as among the breached data on MedStar's computer system.

109. Since the Data Breach, Plaintiff Sanders monitors her financial accounts for about an hour per week. This is more time than she spent prior to learning of the MedStar's Data Breach. Having to do this every week not only wastes her time as a result of MedStar's negligence, but it also causes her great anxiety.

110. Starting since the Data Breach, Plaintiff Sanders began receiving an excessive number of spam calls on the same cell phone number provided to MedStar on her records. These calls are a distraction, must be deleted, and waste time each day. Once the Notice Letter was delivered, and given the timing of the Data Breach, she believes that the calls are related to her stolen PII.

111. In addition, Plaintiff Sanders receives *many* spam emails and texts now, which was not typical before the Data Breach. She cannot figure out any other explanation than that it is related to MedStar's Data Breach which included her Private Information.

112. On approximately April 16, 2024, Plaintiff Sanders experienced an unauthorized charge to her Truist Bank account in the amount of $150.00. Plaintiff Sanders was unable to be reimbursed for this despite disputing it. Due to this fraud, Plaintiff had issues paying other bills, had to make trips to the bank to address the issue, and replaced her bank cards.

113. Plaintiff Sanders is careful with her Private Information and has not experienced fraud before this breach. She believes the unauthorized charges are related to the Data Breach, as there is no other logical explanation given the timeline.

114. Plaintiff Sanders is aware that cybercriminals often sell Private Information, and one stolen, it is likely to be abused months or even years after MedStar's Data Breach.

115. Had Plaintiff Sanders been aware that MedStar's computer systems were not secure, she would not have entrusted MedStar with her PII and PHI.

PLAINTIFF(S)' AND CLASS MEMBERS' INJURIES

172. To date, Defendant MedStar has done absolutely nothing to compensate Plaintiff(s) and Class Members for the damages they sustained in the Data Breach.

173. Defendant MedStar has not even merely offered one year of credit monitoring services. This is a failure to protect the Private Information it allowed to be inadequately safeguarded which has caused Plaintiff(s) and Class great injuries. *See* Ex. A. The lack of services is inadequate when victims are likely to face many years of identity theft.

174. MedStar's offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide

any compensation for its unauthorized release and disclosure of Plaintiff(s)' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

175. Furthermore, Defendant MedStar's credit monitoring offer and advice (*see* Ex. A) to Plaintiff(s) and Class Members squarely places the burden on Plaintiff(s) and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Defendant merely sent instructions to Plaintiff(s) and Class Members about actions they can affirmatively take to protect themselves.

176. Plaintiff(s) and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

177. Plaintiff(s)'and Class Members' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

178. Plaintiff(s) and Class were damaged in that their Private Information is now in the hands of cyber criminals, sold and potentially for sale for years into the future.

179. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

180. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have been forced to expend time dealing with the effects of the Data Breach.

181. Plaintiff(s) and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff(s) and Class

Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

182. Plaintiff(s) and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff(s) and Class Members.

183. Plaintiff(s) and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

184. Plaintiff(s) and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

185. Plaintiff(s) and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

186. Moreover, Plaintiff(s) and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information as well as health information is not accessible online and that access to such data is password-protected.

187. Further, as a result of Defendant's conduct, Plaintiff(s) and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

188. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early

notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, MedStar knew of the breach ***since October 2023*** and did not notify the victims until May, 3, 2024 Yet MedStar offered no explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiff(s) and Class.

CLASS ACTION ALLEGATIONS

189. Plaintiff(s) bring this action on behalf of themselves and on behalf of all other persons similarly situated.

190. Plaintiff(s) propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach discovered by MedStar Health, Inc in 2023 and to whom it provided notice on or about May 2024 (the "Class").

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

192. Plaintiff(s) hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification Fed. R. Civ. P. Rule 23.

193. Numerosity, Fed. R. Civ. P. 23(a)(1): The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is believed to be around 183,079.

194. Commonality. As required by Fed. R. Civ. P. 23(a)(2) and (b)(3), there are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff(s)' and Class Members' Private Information;

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

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

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

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

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

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

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

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

j. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

k. Whether Plaintiff(s) and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

195. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff(s)' claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

196. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiff(s) will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff(s)' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

197. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff(s) and Class Members, in that all the Plaintiff(s)' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

198. Superiority, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying

adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

199. 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.

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

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff(s) and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach;

g. Whether Defendant failed to abide by its responsibilities under HIPAA.

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

CAUSES OF ACTION

First Count
Negligence
(On Behalf of Plaintiff(s) and Class Members)

202. Plaintiff(s) re-alleges and incorporates the above allegations as if fully set forth herein.

203. Defendant MedStar required Plaintiff(s) and Class Members to submit non-public personal information in order to obtain healthcare/medical services and/or employment.

204. By collecting and storing this data in MedStar's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

205. Defendant owed a duty of care to Plaintiff(s) 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.

206. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant MedStar and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

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

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

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

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

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

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

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

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

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

f. 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.

211. 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.

212. 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.

213. Plaintiff(s) and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

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

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

Second Count
Negligence *Per Se*
(On Behalf of Plaintiff(s) and All Class Members)

216. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

217. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff(s)' and Class Members' Private Information.

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

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

220. Defendant breached its duties to Plaintiff(s) and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff(s)' and Class Members' Private Information.

221. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

222. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff(s) and Class Members, Plaintiff(s) and Class Members would not have been injured.

223. The injury and harm suffered by Plaintiff(s) and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known

that it failed to meet its duties, and that Defendant's breach would cause Plaintiff(s) and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

Third Count
Breach of Implied Contract
(On Behalf of Plaintiff(s) and Class Members)

225. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

226. Plaintiff(s) and Class Members provided their Private Information to Defendant MedStar in exchange for Defendant's medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

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

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

229. Plaintiff(s) 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.

230. Plaintiff(s) 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.

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

232. Plaintiff(s) and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

233. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

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

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

236. Plaintiff(s) 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 long-term credit monitoring to all Class Members.

Fourth Count
Breach of Fiduciary Duty
(On Behalf of Plaintiff(s) and Class Members)

237. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

238. In light of the special relationship between Defendant MedStar and Plaintiff(s) and Class Members, whereby Defendant became guardian of Plaintiff(s)' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff(s) and Class Members, (1) for the safeguarding of Plaintiff(s)' and Class Members' Private Information; (2) to timely notify Plaintiff(s) 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.

239. Defendant has a fiduciary duty to act for the benefit of Plaintiff(s) and Class Members upon matters within the scope of its relationship with its current and former patients and employees to keep secure their Private Information.

240. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by failing to diligently discover, investigate, and give detailed notice of the Data Breach to Plaintiff(s) and Class in a reasonable and practicable period of time.

241. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff(s)' and Class Members' Private Information.

242. Defendant breached its fiduciary duties owed to Plaintiff(s) and Class Members by failing to timely notify and/or warn Plaintiff(s) and Class Members of the Data Breach.

243. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by otherwise failing to safeguard Plaintiff(s)' and Class Members' Private Information.

244. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff(s) and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information;

(iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff(s) and Class Members; and (vii) the diminished value of Defendant's services they received.

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

Fifth Count
Unjust Enrichment
(On Behalf of Plaintiff(s) and Class Members)

246. Plaintiff(s) re-allege the above allegations as if fully set forth herein. Plaintiff(s) bring this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of contract count above.

247. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff(s) and the Class Members.

248. As such, a portion of the payments made by or on behalf of Plaintiff(s) 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 Defendant.

249. Plaintiff(s) and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff(s) and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

250. Defendant knew that Plaintiff(s) and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff(s) and Class Members for business purposes.

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

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

253. Defendant failed to secure Plaintiff(s)' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff(s) and Class Members provided.

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

255. If Plaintiff(s) and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

256. Plaintiff(s) and Class Members have no adequate remedy at law.

257. As a direct and proximate result of Defendant's conduct, Plaintiff(s) 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 Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private 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 Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their 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 Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff(s) and Class Members.

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

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

Sixth Count
Declaratory Judgment
(On Behalf of Plaintiff(s) and Class Members)

260. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

261. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

262. An actual controversy has arisen in the wake of the Defendant's Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff(s) and Class members from further data breaches that compromise their Private Information.

263. Plaintiff(s) allege that Defendant's data security measures remain inadequate. Plaintiff(s) will continue to suffer injury because of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

264. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure patients' Private Information and to timely notify patients of a data breach under the common law, HIPAA, Section 5 of the FTC Act, and various states' statutes; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

265. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' Private Information.

266. If an injunction is not issued, Plaintiff(s) and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff(s) and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

267. The hardship to Plaintiff(s) and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at Defendant, Plaintiff(s) and Class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has pre-existing legal obligations to employ such measures.

268. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff(s) and the millions of individuals whose Private Information would be further compromised.

Seventh Count
VIOLATIONS OF THE MARYLAND CONSUMER PROTECTION ACT ("MCPA")
Md. Code Ann., Com. Law § 13-101, *et seq.*

269. Plaintiff(s) reallege and incorporates by reference all preceding paragraphs as if fully set forth herein.

270. The purpose of the Maryland Consumer Protection Act is "to set certain minimum statewide standards for the protection of consumers across the State [of] [Maryland]." Md. Code Ann., Com. Law § 13-102(b)(1).

271. MedStar, Plaintiff(s), and Class members are all "persons" as defined in the MCPA. Md. Code Ann., Com. Law § 13-101(h). Plaintiff and Class members are all "consumers" as defined in the MCPA. Md. Code Ann., Com. Law § 13-101(c).

272. The MCPA prohibits a person from engaging in "any unfair, abusive, or deceptive trade practice" in the sale of goods or services. Md. Code Ann., Com. Law § 13-303.

273. MedStar has violated the Maryland Consumer Protection Act by engaging in the unfair and deceptive practices alleged herein. Pursuant to HIPAA (42 U.S.C. § 1302d *et seq.*), the FTCA, and Maryland law, MedStar was required, but failed, to protect Plaintiff's and Class members' PII/PHI and maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class members' PII/PHI. This constitutes a violation of the Maryland Consumer Protection Act.

274. Further, MedStar has violated the MPIPA, which requires "a business that owns, maintains, or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned, maintained, or licensed and the nature and size of the business and its operations." Md. Code Ann., Com. Law § 14-3503(a).

275. A violation of the MPIPA is "an unfair or deceptive trade practice within the meaning of" the MCPA. Md. Code Ann., Com. Law § 14-3508(1).

276. Plaintiff(s) and Class members seek declaratory judgment that MedStar's data security practices were not reasonable or adequate and caused the cyberattack under the MCPA, as well as injunctive relief enjoining the wrongful acts and practices of MedStar described herein and requiring MedStar to employ and maintain industry accepted standards for data management and security.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff(s) pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff(s) 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 Plaintiff(s)' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff(s) and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to

disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff(s) and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiff(s) demand a trial by jury on all claims so triable.

Dated: May 10, 2024

Respectfully submitted,

/s/ Gary E. Mason
Gary E. Mason
Danielle L. Perry*
Lisa A. White*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: dperry@masonllp.com
Email: lwhite@masonllp.com
Attorneys for Plaintiff(s)

**pro hac vice or applications for admission to be filed*