Exhibit A6

UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

TINA GOLDSMITH, 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: St. Mary's County, MD Plaintiff, v. **MEDSTAR HEALTH, INC.**, Address: 10980 Grantchester Way, 6th Floor, Columbia, MD 21044 County of Residence: Howard County, MD Defendant.	Case No. **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Tina Goldsmith ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through the undersigned attorneys, brings this Class Action Complaint against Defendant MedStar Health, Inc. ("MedStar" or "Defendant"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters as follows.

INTRODUCTION

1. Plaintiff brings this class action against MedStar for its failure to secure and safeguard Plaintiff's and approximately 183,079 other individuals' personally identifiable information ("PII") and personal health information ("PHI"), including patients' names, mailing addresses, dates of birth, dates of service, provider names, and health insurance information.

2. MedStar is a healthcare service provider that operates 10 hospitals and over 300 other locations.

3. Between approximately January 25, 2023 and October 18, 2023, an unauthorized individual or individuals gained access to MedStar's networks and obtained the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. MedStar promised Plaintiff and Class members that it would implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. MedStar breached those promises by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure.

5. As a result of MedStar's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violation of the Maryland Consumer Protection Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Tina Goldsmith

7. Plaintiff Tina Goldsmith is a citizen and resident of Maryland.

8. Plaintiff obtained healthcare services from MedStar. As a condition of receiving services, MedStar required Plaintiff to provide it with her PII/PHI.

9. Based on representations made by MedStar, Plaintiff believed that MedStar had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff provided her PII/PHI to MedStar in connection with and in exchange for receiving healthcare services from MedStar.

10. In connection with providing healthcare services to Plaintiff, MedStar stored and maintained Plaintiff's PII/PHI on their systems, including the system involved in the Data Breach.

11. Had Plaintiff known that MedStar does not adequately protect the PII/PHI in its possession, she would not have agreed to provide MedStar with her PII/PHI or obtained MedStar's healthcare services.

12. Plaintiff received a letter from MedStar notifying her that her PII/PHI was exposed in the Data Breach.

13. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; lost time and money mitigating the effects of the Data Breach; and overpayment for services that did not include adequate data security.

Defendant MedStar Health, Inc.

14. Defendant MedStar Health, Inc., is a Maryland not-for-profit corporation with its headquarters located at 10980 Grantchester Way, 6th Floor, Columbia, MD 21044. It may be served through its registered agent: The Corporation Trust, Inc., 2405 York Road, Suite 201, Lutherville Timonium, MD 21093.

JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

16. This Court has general personal jurisdiction over MedStar because it maintains its principal place of business in this District, regularly conducts business in Maryland, and has sufficient minimum contacts in Maryland.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because MedStar's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of MedStar

18. MedStar "is a $7.7 billion, not-for-profit, regional healthcare system based in Columbia, Maryland."[1] "As the largest healthcare provider in Maryland and the Washington, D.C., region, MedStar Health's more than 300 care locations include 10 hospitals, 33 urgent care clinics, ambulatory care centers, and primary and specialty care providers."[2]

19. In 2023, MedStar had 116,500 inpatient admissions and 5,999,798 outpatient visits.[3]

[1] *Facts and Figures – MedStar Health*, MEDSTAR HEALTH, https://www.medstarhealth.org/about/facts-and-figures (last accessed May 9, 2024).
[2] *Id.*
[3] *Id.*

20. In the regular course of its business, MedStar collects and maintains the PII/PHI of its current and former patients. MedStar required Plaintiff and Class members to provide their PII/PHI as a condition of receiving healthcare services.

21. MedStar's website contains a Patient Privacy Policy (the "Privacy Policy).[4] MedStar notes it is "required to follow the terms of our most current [Privacy Policy]."[5]

22. In the Privacy Policy, MedStar states it "is committed to the protection of your medical information."[6] MedStar admits it is "required by law to maintain the privacy of your health information."[7]

23. The Privacy Policy lists the ways patients' information may be used, including for treatment, payment, and health care operations purposes.[8]

24. The Privacy Policy states patients "have the right to be notified if there is a breach of your health information. A breach means health information is acquired, accessed, used, or disclosed in a manner not permitted by law which causes it to be compromised."[9]

25. MedStar's website also includes a list of patient rights and responsibilities.[10] Among the listed patient rights are the right "[t]o be provided privacy and confidentiality with respect to your personal identity and dignity in care discussions and treatment" and "[t]o have your health information treated confidentially, so that only individuals involved in your care,

---

[4] *Patient Privacy Policy*, MEDSTAR HEALTH (Oct. 30, 2023), https://www.medstarhealth.org/patient-privacy-policy (last accessed May 9, 2024) [hereinafter, "*Privacy Policy*"].
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Patient Rights and Responsibilities*, MEDSTAR HEALTH, https://www.medstarhealth.org/patient-rights-and-responsibilities (last accessed May 9, 2024).

monitoring your quality of care, or otherwise allowed by law will be allowed to access your medical record."[11]

26. Plaintiff and Class members are, or were, patients of MedStar, and entrusted MedStar with their PII/PHI.

The Data Breach

27. Between approximately January 25, 2023 and October 18, 2023, an unauthorized individual, or unauthorized individuals, "accessed emails and files associated with three MedStar Health employee email accounts."[12] An investigation into the Data Breach "determined that patient information was included in the emails and files that were accessed."[13] The PII/PHI accessed in the Data Breach includes "patients' names, mailing address, dates of birth, date(s) of service, provider name(s), and/or health insurance information."[14]

28. According to a data breach notification posted on the Department of Health and Human Services' website, approximately 183,079 individuals' PII/PHI was compromised during the Data Breach.[15]

29. MedStar did not begin to notify impacted breach victims about the data breach until May 3, 2024, over six months after the Data Breach, and two months after learning patient information was compromised.[16] MedStar's failure to promptly notify Plaintiff and Class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who

---

[11] *Id.*
[12] *Notice of Data Incident*, MEDSTAR HEALTH, https://www.medstarhealth.org/notice-of-data-incident (last accessed May 9, 2024).
[13] *Id.*
[14] *Id.*
[15] *Cases Currently Under Investigation*, DEP'T HEALTH & HUM. SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed May 9, 2024).
[16] *See Notice of Data Incident*, *supra* note 12.

exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their PII/PHI will be misused and their identities will be (or already have been) stolen and misappropriated.

MedStar Knew that Criminals Target PII/PHI

30. At all relevant times, MedStar knew, or should have known, that the PII/PHI it collects and maintains was a target for malicious actors. Indeed, MedStar's Privacy Policy indicates it was aware of this risk because it notes it will alert patients if their information is compromised in a data breach.[17] Despite such knowledge, MedStar failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that MedStar should have anticipated and guarded against.

31. It is well known among companies that store sensitive personally identifying information that such information—such as the PII/PHI stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[18]

32. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2024 report, the healthcare compliance company Protenus found that there were

[17] *See Privacy Policy*, *supra* note 4.
[18] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

1,161 medical data breaches in 2023 with over 171 million patient records exposed.[19] This is an increase from the 1,138 medical data breaches which exposed approximately 59 million records that Protenus compiled in 2023.[20]

33. PII/PHI is a valuable property right.[21] The value of PII/PHI as a commodity is measurable.[22] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[23] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[24] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

34. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be

---

[19] *See 2024 Breach Barometer*, PROTENUS 2, https://protenus.com/hubfs/Breach_Barometer/Latest%20Version/Protenus%20-%20Industry%20Report%20-%20Privacy%20-%20Breach%20Barometer%20-%202024.pdf (last accessed May 7, 2024).

[20] *See id*.

[21] *See* Marc van Lieshout, *The Value of Personal Data*, 457 Int'l Fed'n for Info. Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[22] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[23] Organization for Economic Co-operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[24] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

35. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[25] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[26]

36. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[27] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[28]

37. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[29] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted

[25] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[26] *Id.*
[27] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[28] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[29] Steager, *supra* note 25.

disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[30]

38. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[31]

39. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

40. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[32] [33]

41. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other

---

[30] *Id.*

[31] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[32] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed May 7, 2024).

[33] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[34]

42. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[35]

43. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[36] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[37] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [38] The FTC also warns, "If the thief's health information is mixed with yours it

[34] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.
[35] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed May 7, 2024).
[36] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[37] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 28.
[38] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed May 7, 2024).

could affect the medical care you're able to get or the health insurance benefits you're able to use."[39]

44. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [40]

45. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately

[39] *Id*.
[40] *See* Dixon & Emerson, *supra* note 36.

three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[41]

46. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

47. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

48. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

49. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

[41] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

> All persons whose personally identifiable information and personal health information was accessed by unauthorized persons in the Data Breach, including all persons who were sent a notice of the Data Breach.

50. Excluded from the Class are MedStar Health, Inc., and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

51. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

52. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. MedStar has reported to the Department of Health and Human Services that 183,079 persons were affected by the Data Breach.[42]

53. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. whether MedStar had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. whether MedStar had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. whether MedStar failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. whether an implied contract existed between Class members and MedStar, providing that MedStar would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

[42] *See Cases Currently Under Investigation*, *supra* note 15.

e. whether MedStar engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class members;

f. whether MedStar breached their duties to protect Plaintiff's and Class members' PII/PHI; and

g. whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

54. MedStar engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison in both quantity and quality to the numerous common questions that dominate this action.

55. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by MedStar, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

56. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature. Plaintiff has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff and her counsel have adequate resources to assure the interests of the Class will be adequately represented.

57. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against MedStar, so it would be impracticable for

Class members to individually seek redress from MedStar's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

58. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

59. MedStar owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

60. MedStar knew, or should have known, the risks of collecting and storing Plaintiff's and Class members' PII/PHI, and the importance of maintaining secure systems. MedStar knew, or should have known, of the many data breaches that targeted health care providers in recent years.

61. Given the nature of MedStar's business, the sensitivity and value of the PII/PHI its collects and maintain, and the resources at its disposal, MedStar should have identified the vulnerabilities in its systems and prevented the Data Breach from occurring.

62. MedStar breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data

security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

63. It was, or should have been, reasonably foreseeable to MedStar that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

64. But for MedStar's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

65. As a result of MedStar's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

66. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

67. MedStar's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

68. MedStar's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as MedStar, of failing to employ reasonable measures to protect and secure PII/PHI.

69. MedStar's duties also arise from the Maryland Personal Information Protection Act ("MPIPA"), Md. Code Ann., Com. Law § 14-3501, *et seq.*, 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).

70. MedStar violated HIPAA Privacy and Security Rules, Section 5 of the FTCA, and the MPIPA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. MedStar's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores,

and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

71. MedStar's violations of HIPAA Privacy and Security Rules, Section 5 of the FTCA, and the MPIPA constitutes negligence per se.

72. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules, Section 5 of the FTCA, and the MPIPA were intended to protect.

73. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules, Section 5 of the FTCA, and the MPIPA were intended to guard against.

74. It was, or should have been, reasonably foreseeable to MedStar that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

75. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of MedStar's violations of HIPAA Privacy and Security Rules, Section 5 of the FTCA, and the MPIPA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there

is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

76. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

77. Plaintiff and Class members gave MedStar their PII/PHI in confidence, believing that MedStar would protect that information. Plaintiff and Class members would not have provided MedStar with this information had they known it would not be adequately protected. MedStar's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between MedStar and Plaintiff and Class members. In light of this relationship, MedStar must act primarily for the benefit of its current and former patients, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

78. MedStar has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to, or contracting with companies that failed to, properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected and maintained.

79. As a direct and proximate result of MedStar's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of, or imminent threat of, identity theft; (ii) the

compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in MedStar's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

80. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

81. In connection with receiving medical or healthcare services, Plaintiff and all other Class members entered into implied contracts with MedStar.

82. Pursuant to these implied contracts, Plaintiff and Class members paid money to MedStar, whether directly or through their insurers, and provided MedStar with their PII/PHI. In exchange, MedStar agreed to, among other things, and Plaintiff understood that MedStar would: (1) provide medical or health services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

83. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and MedStar, on the other hand. Had Plaintiff

and Class members known that MedStar would not adequately protect its current and former patients' PII/PHI, they would not have sought healthcare services from MedStar.

84. Plaintiff and Class members performed their obligations under the implied contract when they provided MedStar with their PII/PHI and paid—directly or through their insurers—for health care or other services from MedStar.

85. MedStar breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

86. MedStar's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

87. Plaintiff and all other Class members were damaged by MedStar's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk or imminent threat of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity

theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

88. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

89. This claim is pleaded in the alternative to the breach of implied contract claim.

90. Plaintiff and Class members conferred a monetary benefit upon MedStar in the form of monies paid to MedStar for healthcare services, and through the provision of their PII/PHI.

91. MedStar accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. MedStar also benefitted from the receipt of Plaintiff's and Class members' PII, as this was used to facilitate payment.

92. As a result of MedStar's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

93. MedStar should not be permitted to retain the money belonging to Plaintiff and Class members because MedStar failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

94. MedStar should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

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

95. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

96. 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).

97. MedStar, Plaintiff, 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).

98. 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.

99. 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.

100. 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).

101. 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).

102. Plaintiff 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

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide

or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

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

Dated: May 10, 2024

Respectfully submitted,

/s/ *Gary E. Mason*

Gary E. Mason (MD Bar # 15033)
Danielle L. Perry*
Lisa A. White*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290
Email: gmason@masonllp.com
Email: dperry@masonllp.com
Email: lwhite@masonllp.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com

aparkhill@barnowlaw.com

Attorneys for Plaintiff Tina Goldsmith

**Pro hac vice* forthcoming