IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN RE: MEDSTAR HEALTH 2025 DATA SECURITY LITIGATION This Document Relates To: All Actions	Master File No. 1:25-cv-3325-BAH **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Iris Stewart, Richard Foxwell, Nikia Bryant, Brittany Outen, Antoinette Jones, and Tracy Sanders ("Plaintiffs"), individually and on behalf of the Class defined below of similarly situated persons, allege the following against MedStar Health, Inc. ("MedStar" or "Defendant"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by counsel as to all other matters:

SUMMARY OF THE CASE

1. This action arises from Defendant's failure to secure the personal identifiable information ("PII")[1] and protected health information ("PHI")[2] (collectively, "Private

[1] The Federal Trade Commission defines "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." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS.,

Information") of Plaintiffs and the members of the proposed Class, where Plaintiffs provided their Private Information indirectly to Defendant as a condition of receiving care from their medical providers.

2. Defendant MedStar Health operates a healthcare system serving Maryland, Washington, D.C., and parts of Virginia. It operates over 300 hospitals, urgent care centers, physician practices, and specialized clinics and provides full-spectrum medical care to patients across the region.[3] MedStar Health is a $8.3 billion healthcare system and one of the largest employers in the region with more than 35,000 employees.[4] In 2024 alone, MedStar had 6,140,570 outpatient visits and 118,861 inpatient admissions.[5] In the regular course of providing its services, Defendant collects patient information and is fully aware of the sensitivity of that information and its obligation to maintain that information as confidential and safe from unauthorized access.

3. On or about October 4, 2025, a notorious international ransomware gang, Rhysida, publicly claimed credit for accessing and exfiltrating patient data from Medstar. Rhysida represented that they had acquired over 7 million "pieces of patient personal data" from Medstar and posted a seven-day countdown timer and indicated that the data was available for the price of 25 Bitcoin. On December 3, 2025, Defendant finally acknowledged that it discovered, also on

---

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited June 11, 2025).

[3] *See* About, MedStar Health, Inc., https://www.medstarhealth.org/about.

[4] *See also* MedStar Health, Inc. Consolidated Financial Statements and Supplementary Information June 30, 2023, and 2022, https://hscrc.maryland.gov/Documents/Strong%20als%20Folder/Audited%20Financials%20-%20ar-rev/FY%202023/MedStar%20AFS_FY%202023.pdf.

[5] Facts and Figures – MedStar Health, https://www.medstarhealth.org/about/facts-and-figures.

October 4, 2025, that "an outside party gained unauthorized access to MedStar Health's systems that included patient information" (the "Data Breach").[6]

4. The Private Information that Rhysida targeted, accessed, and exfiltrated from Defendant's systems included Plaintiffs' and Class Members' names, dates of birth, Social Security numbers, and information related to their healthcare, including diagnoses, medications, test results, images, health insurance, and treatment information.[7]

5. Defendant could have prevented this Data Breach by implementing reasonable, expected, and industry standard data security measures. Instead, Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement these measures to safeguard its current and former clients' customers' Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. Defendant's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

6. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (f) "out of pocket" costs incurred due to actual identity theft; (g)

---

[6] *See* MedStar Health, *Notice of Data Privacy Incident*, MedStar Health (Dec. 3, 2025), available at https://www.medstarhealth.org/data-incident

[7] *See id*.

decreased credit scores; (h) anxiety, annoyance, and nuisance; and (i) continued risk to their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

7. Plaintiffs and Class Members would not have provided their confidential Private Information had they known that Defendant would, *inter alia*, make their Private Information Internet-accessible, not encrypt personal and sensitive data elements and not delete the Private Information it no longer had reason to maintain.

8. Through this lawsuit, Plaintiffs seek to hold Defendant responsible for the injuries they inflicted on Plaintiffs and Class Members due to their impermissibly inadequate data security measures and seek injunctive relief to ensure the implementation of proper security measures to protect the Private Information that remains in Defendant's possession.

JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of Class Members exceeds 5,000,000 people, many of whom, including several Plaintiffs, have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

10. This Court has personal jurisdiction over Defendant because it is a California limited liability company that operates and has its principal place of business in this District and conducts substantial business in this District.

11. Venue is proper in this Court pursuant to 28 U.S.C. §1391(a)(1) because a substantial part of the vents giving rise to this action occurred in his District. Moreover, Defendant

is domiciled in this District, maintains Plaintiffs' and Class members' Private Information in this District, and has caused harm to Plaintiffs and Class members in this District.

PARTIES

12. Plaintiff Iris Stewart is a natural person and citizen of Baltimore, Maryland, where she intends to remain.

13. Plaintiff Richard Foxwell is a natural person and citizen of Nottingham, Maryland, where he intends to remain.

14. Plaintiff Nikia Bryant is a natural person and citizen of Washington, D.C., where she intends to remain.

15. Plaintiff Brittany Outen is a natural person and citizen of Baltimore, Maryland, where she intends to remain.

16. Plaintiff Antoinette Jones is a natural person and citizen of Catonsville, Maryland, where she intends to remain.

17. Plaintiff Tracy Sanders is a natural person and citizen of Forest Hill, Maryland, where she intends to remain.

18. 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.

FACTUAL ALLEGATIONS

A. Medstar's Business

19. With multiple locations throughout DMV area, Defendant boasts on its website

that "We deliver outstanding care to people experiencing a variety of medical conditions."[8] It touts an annual revenue of $4.4 billion.[9]

20. In collecting and maintaining its current and former patients' Sensitive Information, Defendant agreed it would safeguard the data in accordance with state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information.

21. Indeed, Defendant acknowledges in its Privacy Policy that it "take[s] reasonable measures to protect your information from loss, theft, misuse, unauthorized access, disclosure, alteration, and destruction."[10]

22. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonably cybersecurity safeguards or policies to protect its patients' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Sensitive Information.

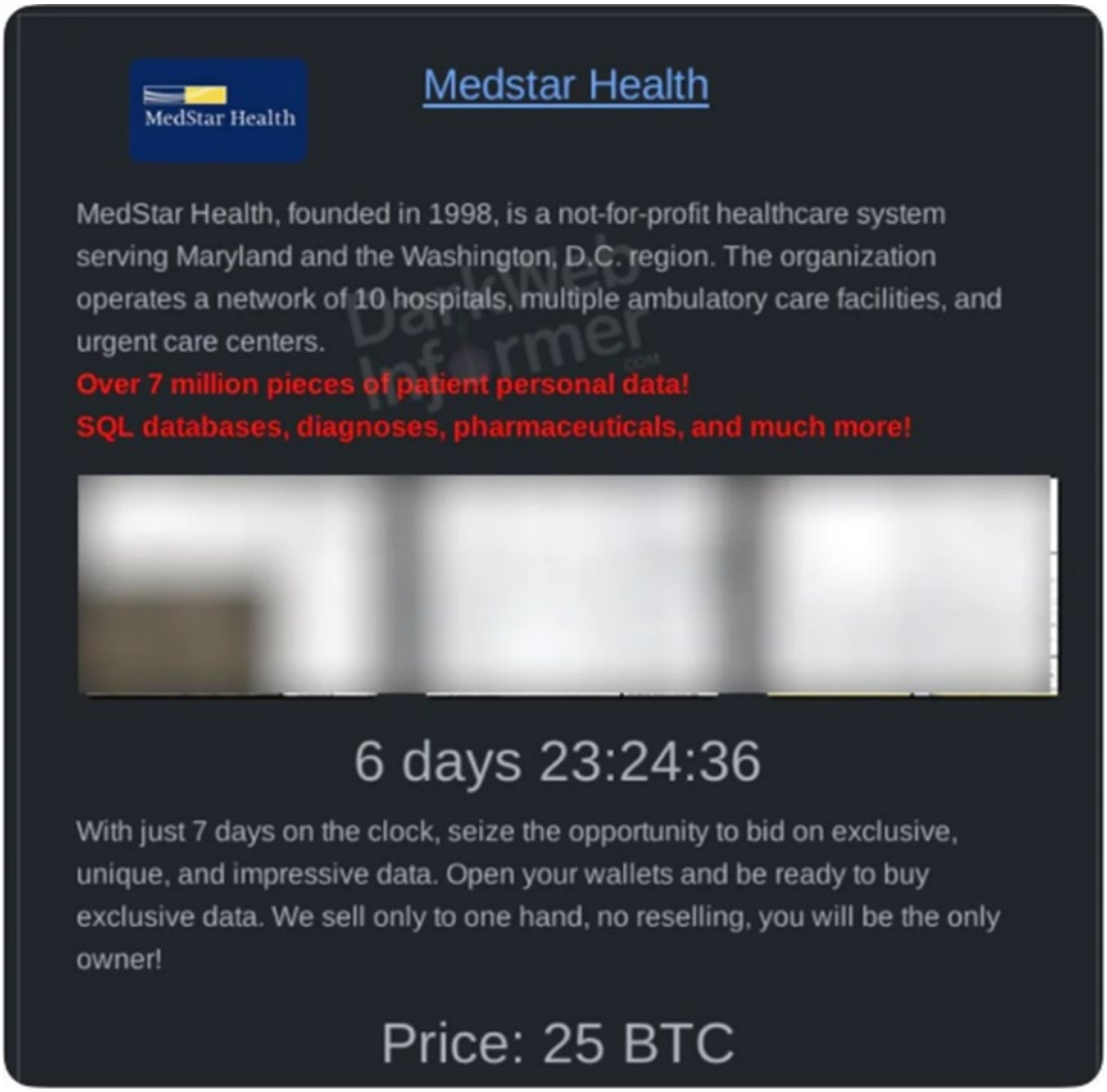
[8] Home, https://www.medstarhealth.org/ (last visited Oct. 8, 2025).

[9] Zoominfo, https://www.zoominfo.com/c/medstar-health/372836681 (last visited Oct. 6, 2025).

[10] Online Privacy Policy, https://www.medstarhealth.org/online-privacy-policy (last visited Oct. 6, 2025).

B. The Data Breach

23. On October 4, Defendant was alerted to the fact that it had been breached and that patient data had been accessed after Rhysidia posted that it had obtained MedStar patient's data. Rhysida used the MedStar logo and described the data as coming from the health care organization, including its hospitals, ambulatory care and urgent care centers. Rhysida also posted a seven-day countdown of the time the data would remain available for sale. It further claimed that it was only selling to "one hand, no reselling," such that the actor who purchased the data would be its exclusive owner.



24. Notably, the seven-day countdown is a familiar tactic of Rhysida after which it makes the information publicly available if no ransom is paid. In 2023, "after the British Library refused to pay a £600,000 ransom, [Rhysida] published close to 500,000 files of what they called 'exclusive, unique and impressive' stolen data for anyone to download for free through the dark web." In November of 2025, "after granting a one-week waiting period, a common tactic for the Rhysida gang, the attackers released a 1.9TB dataset containing over 1.7 million files allegedly belonging to US manufacturing conglomerate Gemini Group."[11] Another cyber security research group noted that "once the auction period ends, Rhysida publicly releases any unsold data on its [dark web site]."[12]

25. Indeed here, following the expiration of the seven-day auction period, Rhysida also made the patient information exfiltrated from MedStar freely available to anyone to access and download, including over 4,300,000 patient SSNs and other information. Because the Private Information available on the dark web includes patient SSNs, medical information, and other immutable identifiers, Plaintiffs and Class Members face a lifetime risk of fraud and identity theft.

26. A ransomware attack is a type of cyberattack that is frequently used to target healthcare providers due to the sensitive patient data they maintain.[13] Ransomware attacks are

---

[11] Cybernews, *Gemini Group Data Leak by Rhysida Ransomware Group* (Dec. 2025), available at https://cybernews.com/security/gemini-group-rhysida-data-leak/

[12] Alexandra Blia & Gal Givon, *From Extortion to E-Commerce: How Ransomware Groups Turn Breaches into Bidding Wars*, **Rapid7** (Nov. 24, 2025), available at https://www.rapid7.com/blog/post/tr-extortion-ecommerce-ransomware-groups-turn-breaches-into-bidding-wars-research/

[13] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/

particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in lengthier patient stays, delayed procedures or test results, increased complications from surgery, and even increased mortality rates.[14] In 2021, 44% of healthcare providers who experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted services for up to a month.[15]

27. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[16] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

28. Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[17] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[18]

---

[14] *Ponemon study finds link between ransomware, increased mortality rate*, available at https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate

[15] *The State of Ransomware in Healthcare 2022*, available at https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf

[16] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[17] *Id*.

[18] *Id*.

29. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[19]

30. Defendant could have prevented or mitigated the consequences of the Data Breach by limiting access to sensitive information to only necessary employees, requiring multi-factor authentication to verify access credentials, encrypting data at rest and in transit, monitoring its systems for signs of unusual activity or the transfer of large volumes of data, and regularly rotating passwords.

31. As evidenced by the Data Breach, the Private Information contained in Defendant's network and was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

32. Defendant's failure to implement these standard and reasonable data security practices resulted in the exfiltration of Plaintiffs and other healthcare patients' sensitive personal and health information.

33. The Notice published by Defendant on December 3, 2025, to Plaintiffs and Class Members states:

> On October 4, 2025, we learned about a cybersecurity incident in which an outside party gained unauthorized access to MedStar Health's systems that included patient information. MedStar immediately took steps to secure our systems, launched an investigation with the assistance of third-party forensic experts, and notified law enforcement. Our investigation determined that the unauthorized access to MedStar Health's systems occurred from September 12, 2025 to September 16, 2025.
>
> On November 12, 2025, we determined that the files accessed by the unauthorized party contained patient information that included

[19] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Nov. 20, 2024).

> patients' names, dates of birth, Social Security numbers, and also potentially other information related to patient care, such as diagnoses, medications, test results, images, health insurance, and treatment information.
>
> We are notifying patients of this incident and sharing the steps that we are taking in response. While we use a number of physical, technical, and administrative controls to ensure the safety and confidentiality of patient information, we continuously review our cybersecurity protections to enhance our safeguards.

34. In the Notice, Defendant offers complimentary identity monitoring services only to patients whose Social Security numbers or driver's license numbers were compromised and nothing in the way of medical monitoring to prevent medical fraud.[20]

35. Moreover, Defendant does not alert victims of the Data Breach that their information has been acquired by a known cybercriminal group or that it has been made available on the dark web after Defendant failed to pay Rhysida's ransom demand.

36. Defendant does not detail the vector of attack or inform Plaintiffs and Class Members whether and how Defendant has implemented additional data security safeguards to protect their Private Information in its continued possession.

37. The Identity Theft Research Center's 2024 Annual Data Breach Report notes that, "approximately 70 percent of cyberattack-related breach notices did not include attack information, compared to 58 percent in 2023. In 2019 and previous years, ~100 percent of breach notices included attack vector information." Eva Velasquez, CEO of the Identity Theft Resource Center, remarked that "[w]ith a near-record number of compromises and over 1.3 billion victim notices, often tied to inadequate cyber practices, we are also seeing an increase in notices that

[20] *See id.*

provide limited actionable information for victims."[21]

38. Despite Defendant's attempt to obfuscate the details of the Data Breach, it is clear that Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, such as encrypting the information or purging it when it is no longer needed, causing the exposure of Private Information.

C. Data Breaches are Foreseeable and Preventable

39. Data breaches are preventable.[22] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[23] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[24]

40. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. Data breaches have been on the rise for several years. In 2023

---

[21] Identity Theft Resource Center, *2024 Annual Data Breach Report Reveals Near-Record Number of Compromises and Victim Notices*, ITRC (Jan. 28, 2025), available at https://www.idtheftcenter.org/post/2024-annual-data-breach-report-near-record-compromises/

[22] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.

[23] *Id.* at 17.

[24] *Id.* at 28.

there were 3,205 compromises affecting 353,027,892 total victims. The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1,400 percentage points. "In 2024, healthcare data breaches reached an all-time high, with 276,775,457 records compromised – a 64.1% increase from the previous year's record and equivalent to 81.38% of the United States population."[25]

41. In light of recent high profile data breaches at other healthcare organizations, including Yale New Haven Health (5.5 million records, April 2025), Episource, LLC (5.4 million records, June 2025), Blue Shield of California (4.7 million records, May 2025), Frederick Health Medical Group (934,326 records, February 2025), University of Pittsburgh Medical Center (712,000 records, March 2025), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

42. Moreover, this is at least the third time MedStar has been the subject of a data breach. In 2016, a ransomware attack forced MedStar to shut down its computers at all ten of its hospitals while the hacker demanded a ransom in the form of bitcoin payment.[26] MedStar had to operate on paper when handling medical records and prescriptions for patients that they were

[25] Cybernews, *US Hospitals and Health Systems Data Breach* (Apr. 8, 2025), available at https://cybernews.com/security/us-hospitals-and-health-systems-data-breach/

[26] Pete Williams, *MedStar Hospitals Recovering After 'Ransomware' Hack, NBC News* (Mar. 31, 2016), https://www.nbcnews.com/news/us-news/medstar-hospitals-recovering-after-ransomware-hack-n548121; MedStar Hack Shows Risks that Come with Electronic Health Records, Aug. 19, 2019, https://www.baltimoresun.com/2016/04/02/medstar-hack-shows-risks-that-come-with-electronic-health-records/?clearUserState=true.

seeing during the shutdown, which lasted days.[27] In 2024, MedStar notified its patients and employees that someone had gained unauthorized access to three MedStar Health employee email accounts, compromising the records of approximately 184,000 individuals.[28] Additionally, in March of this year, MedStar Saint Mary patient records, including SSNs, and medical records, were acquired by threat actors who exploited a vulnerability in its IT partner's software.[29]

43. Additionally, the threat from Rhysdia itself was foreseeable as the U.S. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Multi-State Information Sharing and Analysis Center issued an alert about Rhysida, the cybercriminals responsible for this Data Breach, in November 2023.[30] The warning disseminated key information about the ransomware group including indicators of compromise, detection methods, tactics, techniques, and procedures used.[31] The warning also alerted the public that Rhysida has in the past targeted organizations in education, manufacturing, information technology and government

---

[27] Pete Williams, MedStar Hospitals Recovering After 'Ransomware' Hack, NBC News (Mar. 31, 2016), https://www.nbcnews.com/news/us-news/medstar-hospitals-recovering-after-ransomware-hack-n548121

[28] Suzanne Smalley, *Nearly 184,000 MedStar Health Patients' Personal Data Possibly Breached*, The Record (May 7, 2024), https://therecord.media/medstar-health-data-breach

[29] MedStar Health, *Notice of Oracle Health Data Security Incident* (Mar. 15, 2025), available at https://www.medstarhealth.org/-/media/project/mho/medstar/hospitals/pdf/substitute-notice_website-posting.pdf

[30] *CISA, FBI, and MS-ISAC Release Advisory on Rhysida Ransomware*, Cybersecurity & Infrastructure Security Agency (Nov. 15, 2023), https://www.cisa.gov/news-events/alerts/2023/11/15/cisa-fbi-and-ms-isac-release-advisory-rhysida-ransomware (last visited Dec. 9, 2024).

[31] *Id.*

sectors. [32] Security researchers also warned in 2024 that "[h]ospitals and other healthcare providers have been frequent targets [of Rhysida] due to the sensitive nature of patient data and the potential disruption to critical services.[33]

44. And, as organizations became more dependent on computer systems to run their business,[34] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[35]

45. MedStar recognizes its own obligation to implement reasonable data security safeguards, and its website includes a "Notice of Privacy Practices for MedStar Health stating that Medstar is "required by law to maintain the privacy of your health information and to give you this Notice of our legal duties, our privacy practices, and your rights. We are required to follow the terms of our most current Notice. When we disclose information to other persons and companies to perform services for us, we will require them to protect your privacy."[36]

46. MedStar further acknowledges that there are multiple privacy laws governing their obligation to protect and disclose any sharing of patient data. MedStar states in its Privacy Policy

---

[32] *Id.*

[33] Red Piranha, *Threat Intelligence Report: September 24 – 30, 2024* (Sept. 30, 2024), available at https://redpiranha.net/news/threat-intelligence-report-september-24-september-30-2024

[34] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[35] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

[36] Patient Privacy Policy, Notice of Privacy Policy for MedStar Health, Amended Oct. 30, 2023, https://www.medstarhealth.org/patient-privacy-policy.

that "[t]here are other laws we are required to follow that may provide additional protections, such as laws related to mental health, behavioral health, alcohol and other substance abuse, genetic information, and communicable disease or other health conditions."[37]

47. MedStar also states that in the event that it shares information with other healthcare entities, it would "facilitate the secure exchange of your electronic health information."[38]

48. MedStar further states that it has an obligation to notify its patients if there is a breach of the patient's health information. "You 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."[39]

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

50. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in Defendant's possession and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

D. Defendant Failed to Comply with Regulatory Requirements and Standards.

51. Federal and state regulators have established security standards and issued

---

[37] *Id.*

[38] *Id.*

[39] *Id.*

recommendations to prevent data breaches and the resulting harm to consumers. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

52. The Federal Trade Commission ("FTC") has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[40]

53. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[41]

54. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

55. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented

---

[40] *Start With Security*, Fed. Trade Comm'n ("FTC"), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 11, 2025).

[41] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/system/files/ documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 11, 2025).

reasonable security measures.[42]

56. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

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

58. Defendant's failure to verify that it had implemented reasonable security measures constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. Furthermore, Defendant is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

60. The Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

---

[42] *Id.*

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.[43]

61. Pursuant to HIPAA's mandate that Defendant follows "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302, Defendant was required to, at minimum, "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

62. Defendant is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

63. Both HIPAA and HITECH obligate Defendant to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

64. Defendant has failed to comply with HIPAA and HITECH. It has failed to maintain

---

[43] *Summary of the HIPAA Security Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited June 11, 2025).

adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of PHI.

E. Defendant Failed to Comply with Industry Practices.

65. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[44] All organizations collecting and handling Private Information, such as Defendant, are strongly encouraged to follow these controls.

66. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting of physical security systems; protecting against any possible communication system; and training staff regarding critical points.[45]

67. Other best practices include but are not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, limiting access to sensitive information to only necessary employees,

---

[44] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited June 11, 2025).

[45] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security (last visited June 11, 2025).

and securing application software.[46]

68. The following frameworks incorporate these data security measures and others and are regularly employed as industry standard practices: the NIST Cybersecurity Framework 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

69. Defendant failed to follow these and other industry standards to adequately protect the Private Information of Plaintiffs and Class Members.

F. The Data Breach Caused Injury to Class Members and Will Result in Additional Harm Such as Fraud.

70. The ramifications of Defendant's failure to secure Plaintiffs' and Class Members' data are severe. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. The ramifications of Defendant's failure to secure Plaintiffs' and Class Members' data are severe. Moreover, as a result of Defendant's delay between detecting the Data Breach in February of 2025, and the notice of the Data Breach sent to affected persons in June, the risk of fraud for Plaintiffs and Class Members increased exponentially.

71. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[47] The FTC describes "identifying

[46] *See* Center for Internet Security, *Critical Security Controls* (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited June 11, 2025).

[47] 17 C.F.R. § 248.201 (2013).

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[48]

72. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here.[49] The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the Internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[50] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[51]

73. When the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [Private Information] belonging to victims from countries all over the world. One of the key challenges of protecting Private Information online is

---

[48] *Id*.

[49] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

[50] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[51] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

its pervasiveness. As data breaches in the news continue to show, Private Information about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[52]

74. Identity thieves can use the Private Information that Defendant failed to keep secure to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud, such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

75. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[53]

76. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a 's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60

[52] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited June 11, 2025).

[53] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

or $70."[54] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[55]

77. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[56]

78. The "high value of medical records on the dark web has surpassed that of social

---

[54] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[55] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[56] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

security and credit card numbers. These records can sell for up to $1,000 online."[57]

79. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[58] (Emphasis added).

80. 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. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[59]

81. The Social Security Administration further stresses that:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your

---

[57] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[58] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[59] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

> name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[60]

82. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[61]

83. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[62]

84. According to national credit bureau Experian:

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

---

[60] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[61] *Hackers Stole Consumers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, *available at:* https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-consumers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658 (last visited July 31, 2023).

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

85. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[63] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[64]

86. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in by the New York Times.[65]

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

88. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n 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 has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt

---

[63] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-consumers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited Feb. 21, 2023).

[64] *Id.*

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

to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[66]

89. Even if stolen Private Information does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to target them with spam emails or solicitations to deceive the victim into providing the criminal with additional personal information.

90. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[67]

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

---

[66] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

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

individuals.

92. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

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

94. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

95. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that people lost approximately $18.7 million to such scams in 2023 alone.[68]

96. Accordingly, providing credit monitoring or reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims

[68] *Internet Crime Report*, FEDERAL BUREAU OF INVESTIGATION, (2023), https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf scams.

must spend numerous hours and their own money repairing the impact to their credit. Javelin Research reported that "[f]raud-related resolution hours skyrocketed in 2023. The average amount of time consumers spent in 2022 resolving issues stemming from identity fraud clocked in at six hours, but in 2023, fraud resolution hours rose steeply, jumping to a nearly 10-hour average, a major disruption for consumers and financial institutions alike."[69]

97. Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting credit bureaus to place a fraud alert, reviewing their credit reports, placing a credit freeze on their credit, and correcting their credit reports.[70] The result is that Plaintiffs and Class Members are forced to spend their own personal time, or take time from work, to respond to the Data Breach and Defendant has not offered to compensate them for this loss of time.

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

---

[69] *Javelin Strategy & Research, 2024 Identity Fraud Study: Resolving the Shattered Identity Crisis* (2024), available at https://javelinstrategy.com/research/2024-identity-fraud-study-resolving-shattered-identity-crisis.

[70] *See* https://www.identitytheft.gov/Steps.

99. Because the information stolen in the Data Breach is immutable and cannot be changed, it can be used to perpetrate fraud and identity theft for the remainder of their lives. Plaintiffs and Class Members now face years of constant surveillance of their financial and medical records, monitoring, and loss of rights.

G. Plaintiffs and Class Members Suffered Damages.

100. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation.

101. As a direct and proximate result of Defendant's failure to protect the Private Information, Plaintiffs and the Class have been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Private Information, resulting in ongoing monetary loss and economic harm, loss of value of Private Information, loss of privacy and confidentiality of the stolen Private Information, illegal sales of the compromised Private Information on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, lost work time, and other injuries.

102. Information regarding an individual's health and medical choices, such as here, are some of the most personal and private types of information that exist. An individual's right to privacy regarding their body, their medical care, and their reproductive choices are some of the most sacrosanct and inviolable rights an individual can possess. Damages relating to an individual's loss of privacy and dignitary harm has also long been recognized as recoverable by courts and in the common law.

103. Because personal data is valuable personal property, market exchanges now exist where Internet users like Plaintiffs and Class Members can sell or monetize their own personal data. The data brokering industry was worth roughly $303 billion in 2024 and projected to expand to $332.89 billion in 2025.[71] In fact, the data marketplace is so sophisticated that patients can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[72,73] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[74]

104. Moreover, the value of Private Information is, in part, derived from its confidentiality. Consumers realize the value of Private Information by using it to verify their identities, apply for employment, and secure financial products at favorable rates. When the integrity of this data is compromised, its utility is diminished and its value is lost.

105. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has

---

[71] *See Data Broker Industry Analysis Report 2025: Trends and Revenue Projections by Data Types, Pricing Models, Applications, End-Users and Regional Markets to 2034*, GlobeNewswire (Aug. 20, 2025), available at https://www.globenewswire.com/news-release/2025/08/20/3136224/0/en/Data-Broker-Industry-Analysis-Report-2025-Trends-and-Revenue-Projections-by-Data-Types-Pricing-Models-Applications-End-Users-and-Regional-Markets-to-2034.html

[72] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[73] https://datacoup.com/

[74] https://digi.me/what-is-digime/

been lost, thereby causing additional loss of value.

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

a. theft and misuse of their personal, medical, and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and misused via the sale of Plaintiffs' and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. 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;

g. ascertainable losses in the form of diminution of the value of their Private Information, for which there is a well-established national and international market;

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience,

nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

i. nominal damages.

107. While Plaintiffs' and Class Members' Private Information has been stolen, Defendant continues to hold Plaintiffs' and Class Members' Private Information. Particularly because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and Class Members have an undeniable interest in ensuring that their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

H. Plaintiffs' Experiences

Plaintiff Iris Stewart

108. Plaintiff Iris Stewart is a patient of Defendant and a Data Breach victim.

109. As a condition of receiving services with MedStar, Plaintiff Stewart provided Defendant with her Private Information. Defendant used that Private Information to facilitate its services to Plaintiff and required Plaintiff to provide that Private Information to obtain healthcare services.

110. Plaintiff Stewart provided her Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

111. Defendant deprived Plaintiff Stewart of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Breach.

112. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Stewart's Private Information for theft by cybercriminals and sale on the dark web.

113. Plaintiff Stewart's Private Information has already been published by

cybercriminals on the Dark Web.

114. Plaintiff Stewart suffered actual injury from the exposure of her Private Information —which violates her rights to privacy. Plaintiff Stewart's Social Security number and other Private Information are among the data exfiltrated from MedStar and now available to download from Rhysida's dark web site.

115. Plaintiff Stewart suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

116. Following the Data Breach, Plaintiff Stewart began suffering a significant increase in spam calls, emails, and texts. These spam calls and texts again suggest that her Private Information is now in the hands of cybercriminals.

117. Further and also following the Data Breach, Plaintiff Stewart was forced to close out her Navy Federal account due to numerous suspicious activity. This suspicious activity is further evidence that her Private Information is now in the hands of cybercriminals.

118. Once an individual's Private Information is for sale and access on the dark web, cybercriminals are able to use the stolen and compromised information to gather and steal even more information.[75] On information and belief, the spam texts, emails, and calls as well as the suspicious activity on her Navy Federal account are a result of the Data Breach.

119. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, dealing with spam communications, and self-monitoring her accounts and credit reports to ensure

[75] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information.

no fraudulent activity has occurred.

120. Plaintiff Stewart has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. This is valuable time she would have otherwise spent on other activities, including but not limited to, work and/or recreation

121. Plaintiff Stewart fears for her personal financial security and uncertainty over what Private Information was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

122. Plaintiff Stewart is now subject to the present and continuing substantially increased risk of fraud, identity theft, and misuse for her lifetime resulting from her Private Information being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff Stewart about the Data Breach in a timely fashion.

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

Plaintiff Richard Foxwell

124. Plaintiff Richard Foxwell is a patient of Defendant and a Data Breach victim, having received a Notice Letter dated May 3, 2024.

125. As a condition of receiving services from MedStar, Plaintiff Foxwell provided Defendant with his Private Information, including but not limited to his name, mailing address, date of birth, date(s) of service, provider name(s), and health insurance information. Defendant used that Private Information to facilitate its services to Plaintiff and required Plaintiff to provide

that Private Information to obtain healthcare services.

126. Plaintiff Foxwell provided his Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

127. Defendant deprived Plaintiff Foxwell of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him about the Breach.

128. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Foxwell's Private Information for theft by cybercriminals and sale on the dark web.

129. Plaintiff Foxwell's Private Information has already been published by cybercriminals on the Dark Web. Plaintiff Foxwell's Social Security number and other Private Information are among the data exfiltrated from MedStar and now available to download from Rhysida's dark web site.

130. Plaintiff Foxwell suffered actual injury from the exposure of his Private Information —which violates his rights to privacy.

131. Plaintiff Foxwell suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

132. As a result of the Data Breach, Plaintiff Foxwell has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and monitoring his accounts.

133. Plaintiff Foxwell has already spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. This is valuable time he would have otherwise spent on other activities, including but not limited to, work and/or recreation

134. Plaintiff fears for his personal financial security and uncertainty over what Private

Information was exposed in the Data Breach. Plaintiff Foxwell has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

135. Plaintiff Foxwell is now subject to the present and continuing substantially increased risk of fraud, identity theft, and misuse for his lifetime resulting from his Private Information being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach in a timely fashion.

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

Plaintiff Nikia Bryant

137. Plaintiff Nikia Bryant is a patient of Defendant and a Data Breach victim.

138. As a condition of receiving services from MedStar, Plaintiff Bryant provided Defendant with her Sensitive Information, including but not limited to her name, debit card information that she has used for co-pays throughout the year, address, emergency contact information, and health information. Defendant used that Sensitive Information to facilitate its services to Plaintiff and required Plaintiff to provide that Sensitive Information to obtain healthcare services.

139. Plaintiff Bryant provided her Sensitive Information to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

140. Defendant deprived Plaintiff Bryant of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Breach.

141. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Bryant's Sensitive Information for theft by cybercriminals and sale on the dark web.

142. Plaintiff Bryant's Sensitive Information has already been published by cybercriminals on the Dark Web. Plaintiff Bryant's Social Security number and other Private Information are among the data exfiltrated from MedStar and now available to download from Rhysida's dark web site. Moreover, Plaintiff Bryant's credit monitoring services indicated that she was a victim of this Data Breach.

143. Plaintiff Bryant suffered actual injury from the exposure of her Sensitive Information—which violates her rights to privacy.

144. Plaintiff Bryant suffered actual injury in the form of damages to and diminution in the value of her Sensitive Information. After all, Sensitive Information is a form of intangible property—property that Defendant was required to adequately protect.

145. Following the Data Breach, Plaintiff Bryant was notified by the IRS that an unauthorized actor filed a false tax return in her name, delaying her tax refund and forcing her to spend significant time remediating the issue.

146. As a result of the Data Breach, Plaintiff Bryant has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, monitoring credit card and financial account statements daily, making calls to the IRS to resolve the fraudulent tax filing.

147. Plaintiff Bryant has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. This is valuable time she would have otherwise spent on other activities, including but not limited to, work and/or recreation.

148. Plaintiff Bryant fears for her personal financial security and uncertainty over what

Sensitive Information was exposed in the Data Breach. Plaintiff Bryant has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

149. Plaintiff Bryant is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff Bryant about the Data Breach in a timely fashion.

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

Plaintiff Brittany Outen

151. Plaintiff Brittany Outen is a patient of Defendant and a Data Breach victim.

152. As a condition of receiving services from MedStar, Plaintiff Outen provided Defendant with her Private Information, including but not limited to her name, Social Security number, date of birth, name, address, and medical history. Defendant used that Private Information to facilitate its services to Plaintiff and required Plaintiff to provide that Private Information to obtain healthcare services.

153. Plaintiff Outen provided her Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

154. Defendant deprived Plaintiff Outen of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Breach.

155. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Outen's

Private Information for theft by cybercriminals and sale on the dark web.

156. Plaintiff Outen's Private Information has already been published by cybercriminals on the Dark Web. Plaintiff Outen's Social Security number and other Private Information are among the data exfiltrated from MedStar and now available to download from Rhysida's dark web site.

157. Plaintiff Outen suffered actual injury from the exposure of her Private Information—which violates her rights to privacy.

158. Plaintiff Outen suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

159. As a result of the Data Breach, Plaintiff Outen has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and monitoring her credit information.

160. Plaintiff Outen has already spent and will continue to spend time and effort monitoring her accounts to protect herself from identity theft. This is valuable time she would have otherwise spent on other activities, including but not limited to, work and/or recreation.

161. Plaintiff Outen fears for her personal financial security and uncertainty over what Private Information was exposed in the Data Breach. Plaintiff Outen has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

162. Plaintiff Outen is now subject to the present and continuing substantially increased risk of fraud, identity theft, and misuse for her lifetime resulting from her Private Information

being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff Outen about the Data Breach in a timely fashion.

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

Plaintiff Antoinette Jones

164. Plaintiff Antoinette Jones is a patient of Defendant and a Data Breach victim.

165. As a condition of receiving services from MedStar, Plaintiff Jones provided Defendant with her Sensitive Information, including but not limited to her name, address, email address, phone number, Social Security number, health diagnosis information, and ID information. Defendant used that Sensitive Information to facilitate its services to Plaintiff and required Plaintiff to provide that Sensitive Information to obtain healthcare services.

166. Plaintiff Jones provided her Sensitive Information to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

167. Defendant deprived Plaintiff Jones of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Breach.

168. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Jones's Sensitive Information for theft by cybercriminals and sale on the dark web.

169. Plaintiff Jones's Sensitive Information has already been published by cybercriminals on the Dark Web. Plaintiff Jones's Social Security number and other Private Information are among the data exfiltrated from MedStar and now available to download from Rhysida's dark web site.

170. Plaintiff Jones suffered actual injury from the exposure of her Sensitive Information —which violates her rights to privacy.

171. Plaintiff Jones suffered actual injury in the form of damages to and diminution in the value of her Sensitive Information. After all, Sensitive Information is a form of intangible property—property that Defendant was required to adequately protect.

172. Following the Data Breach, Plaintiff Jones was notified by Credit Karma that a credit account was unauthorizedly opened in her name. Unauthorized charges of $300 were made on the account, forcing Plaintiff to spend time closing the account and disputing the charges.

173. Additionally, since the Data Breach, Plaintiff Jones discovered that an unauthorized actor has been using her medical insurance and as a result she has been receiving bills for missed payments.

174. As a result of the Data Breach, Plaintiff Jones has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, resolving the unauthorized charges on the credit account opened in her name, downloading anti-malware software, and spending time on the phone with MedStar to resolve fraudulent use of her insurance.

175. Plaintiff Jones has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. This is valuable time she would have otherwise spent on other activities, including but not limited to, work and/or recreation.

176. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach. Plaintiff Jones has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data

Breach victim that the law contemplates and addresses.

177. Plaintiff Jones is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach in a timely fashion.

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

Plaintiff Tracy Sanders

179. Plaintiff Tracy Sanders is a patient of Defendant and a Data Breach victim.

180. As a condition of receiving services from MedStar, Plaintiff Sanders provided Defendant with her Private Information, including but not limited to her name, Medical Record number, insurance provider information, driver's license number, Social Security number, email address, financial account numbers, and phone number. Defendant used that Private Information to facilitate its services to Plaintiff Sanders and required Plaintiff to provide that Private Information to obtain healthcare services.

181. Plaintiff Sanders provided her Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

182. Defendant deprived Plaintiff Sanders of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify him about the Breach.

183. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Sanders's Private Information for theft by cybercriminals and sale on the dark web.

184. Plaintiff Sanders' Private Information has already been published by cybercriminals on the Dark Web. Plaintiff Sanders' Social Security number and other Private Information are among the data exfiltrated from MedStar and now available to download from Rhysida's dark web site.

185. Plaintiff Sanders suffered actual injury from the exposure of her Private Information—which violates her rights to privacy.

186. Plaintiff Sanders suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

187. Following the Data Breach, Plaintiff Sanders has suffered from approximately nine unrecognized hard inquiries on her credit from credit card companies with which she has no affiliation. As a result of these unauthorized inquiries, her credit score dropped from the 600 range to approximately 499. Both Equifax and TransUnion advised her to lock her credit reports to prevent further unauthorized activity.

188. Additionally, since the Data Breach, Plaintiff Sanders began suffering a significant increase in spam calls and text messages. The spam callers frequently attempt to scam Plaintiff into providing them with her financial account information and claim that she owes money for purported debts that she did not incur. Additionally, Plaintiff receives approximately 12 spam text messages per day, which include requests for payment of bills she does not owe, notices about insurance premiums she never agreed to, and credit card inquiries which she did not authorize. These spam calls and texts suggest that her Private Information is now in the hands of cybercriminals.

189. Once an individual's Private Information is for sale and access on the dark web, cybercriminals are able to use the stolen and compromised information to gather and steal even more information.[76] On information and belief, the spam texts, emails, and calls as well as the suspicious activity on her credit report are a result of the Data Breach.

190. As a result of the Data Breach, Plaintiff Sanders has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, monitoring her credit information, communicating with Equifax and TransUnion regarding credit inquiries and locking her credit, and dealing with spam text messages and phone calls.

191. Plaintiff Sanders has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. So far, she has spent approximately five hours dealing with the Data Breach. This is valuable time she would have otherwise spent on other activities, including but not limited to, work and/or recreation.

192. Plaintiff Sanders fears for her personal financial security and uncertainty over what Private Information was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

193. Plaintiff Sanders is now subject to the present and continuing substantially increased risk of fraud, identity theft, and misuse for her lifetime resulting from her Private Information being placed in the hands of unauthorized third parties. This injury was worsened by

[76] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited Nov. 24, 2025).

Defendant's failure to inform Plaintiff about the Data Breach in a timely fashion.

194. Plaintiff Sanders has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected.

CLASS ALLEGATIONS

195. Plaintiffs bring this action on behalf of themselves, and all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a) and (b) (the "Nationwide Class"):

> All persons residing in the United States whose Private Information was accessed in the Data Breach, including all who were sent a notice of the Data Breach

196. Plaintiffs Stewart, Foxwell, Outen, Jones, Sanders ("Maryland Plaintiffs") separately seek to represent a Maryland Subclass defined as:

> All persons residing in the state of Maryland whose Private Information was accessed in the Data Breach, including all who were sent a notice of the Data Breach.

197. Plaintiff Bryant separately seeks to represent an Illinois Subclass defined as:

> All persons residing in Washington D.C. whose Private Information was accessed in the Data Breach, including all who were sent a notice of the Data Breach.

198. Excluded from the Class and Subclasses are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which Defendant has a controlling interest, as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s).

199. Plaintiffs reserve the right to modify or amend the foregoing Class definitions before the Court determines whether certification is appropriate.

200. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable.

201. Commonality and Predominance: Common questions of law and fact exist as to all

Class Members and predominate over any potential questions affecting only individual Class Members. These common questions of law or fact include, *inter alia*:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

c. Whether Defendant's computer systems and data security practices used to protect Plaintiffs' and Class Members' Private Information violated the FTC Act, HIPAA, and/or state laws, and/or Defendant's other duties discussed herein;

d. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class Members;

e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

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

h. Whether Plaintiffs and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

i. Whether Defendant failed to exercise reasonable care to secure and

safeguard Plaintiffs' and Class Members' Private Information;

j. Whether Defendant breached duties to protect Plaintiffs' and Class Members' Private Information;

k. Whether Defendant's actions and inactions alleged herein were negligent;

l. Whether Defendant were unjustly enriched by their conduct as alleged herein;

m. Whether Plaintiffs and Class Members were intended third party beneficiaries of contracts between Defendant and its clients, pursuant to which Defendant was required to protect Plaintiffs' and Class Members' Private Information and privacy, and whether that contract was breached;

n. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages or other relief, and the measure of such damages and relief;

o. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

p. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

202. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves 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.

203. Typicality: Plaintiffs 'claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their Private Information compromised in the Data Breach.

Plaintiffs and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

204. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs are an adequate representative of the Class and has no interests adverse to, or conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

205. Superiority: 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 detriments suffered by Plaintiffs and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class Members to individually seek redress from Defendant'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.

206. Injunctive and Declaratory Relief: Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

207. All members of the proposed Class are readily ascertainable. Defendant has access

to the names in combination with addresses and/or e-mail addresses of Class Members affected by the Data Breach. Indeed, impacted Class Members already have been preliminarily identified and sent a breach notice letter.

CAUSES OF ACTION
COUNT I
NEGLIGENCE AND NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Nationwide Class)

208. Plaintiffs restate and reallege the preceding paragraphs as if fully set forth herein.

209. Defendant requires its client's customers to submit non-public Private Information as a condition of risk adjustment services, software, and solutions. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business, which affects commerce.

210. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that the information would be safeguarded against the foreseeable threat of a cyberattack designed to acquire that information.

211. Defendant knew and understood that cyberattacks are a foreseeable risk against which it was required to protect. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if their Private Information were wrongfully disclosed.

212. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

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

Private Information.

214. Defendant also had a duty to exercise appropriate clearinghouse practices to remove its former clients' customers' Private Information they were no longer required to retain pursuant to regulations.

215. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach, but failed to do so.

216. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiffs and Class Members, on the other hand. That special relationship arose because Defendant was entrusted with their confidential Private Information as a condition of receiving risk adjustment services, software, and solutions with Defendant.

217. Defendant had duties arising under the FTC Act and HIPAA to protect Plaintiffs' and Class Members' Private Information.

218. Defendants' violations of Section 5 of the FTC Act and HIPAA (and similar state statutes) constitute negligence per se.

219. Plaintiffs and Class Members are consumers within the class of persons that these statutes were intended to protect and the harm that has occurred is the type of harm these statutes were intended to guard against.

220. In addition, under state data security and consumer protection statutes such as those outlined herein, Defendant had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information.

221. Plaintiffs and Class Members were foreseeable victims of Defendant's violations of the FTC Act and HIPAA, and state data security and consumer protection statutes. Defendant

knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' Private Information would cause damage to Plaintiffs and the Class.

222. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described herein, but also because Defendant is bound by industry standards to protect confidential Private Information. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain pursuant to regulations.

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

224. Defendant had and continues to have duties to adequately disclose that Plaintiffs' and Class Members' Private Information within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

225. Defendant breached its duties and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and 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 for unauthorized access or the transfer of large volumes of data;

c. Failing to encrypt or limit access to Class Members' Private Information;

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

e. Failing to remove former clients' customers' Private Information they were no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

226. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

227. Defendant knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' Private Information would cause damage to Plaintiffs and the Class.

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

229. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in

collecting and storing Private Information, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on its systems.

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

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

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

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

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

235. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiffs' and Class Members' Private Information, and the harm, or risk of imminent harm suffered by Plaintiffs and the Class. Private Information was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care by adopting, implementing, and maintaining appropriate security measures.

236. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by the Data Breach; (x) the value of the unauthorized access to their Private Information permitted by Defendant; and (xi) any nominal damages that may be awarded.

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

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

239. Defendant's negligent conduct is ongoing, in that it still possesses Plaintiffs' and Class Members' Private Information in an unsafe and insecure manner.

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

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

241. Plaintiffs restate and reallege the preceding paragraphs as if fully set forth herein.

242. Plaintiffs and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining health care services provided by Defendant. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for health care services.

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

244. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

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

246. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

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

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

249. Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

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

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

252. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

253. Plaintiffs and Class Members would not have entrusted their Private Information to

Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

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

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

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

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

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

258. Plaintiffs restate and reallege the preceding paragraphs as if fully set forth herein.

259. This count is brought in the alternative to Plaintiffs' breach of implied contract count.

260. Plaintiffs and Class Members conferred a monetary benefit on Defendant through payments made to Defendant directly or on their behalf. In addition, they provided Defendant with their Private Information. In exchange, Defendant should have provided adequate data security for Plaintiffs' and Class Members' Private Information.

261. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the

form of payments made on their behalf by their healthcare organizations and through the receipt of their Private Information as a necessary part of providing its services. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

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

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

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

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

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

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

268. Defendant enriched itself by saving the costs it reasonably should have expended

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

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

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

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

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

COUNT IV
MARYLAND PERSONAL INFORMATION PROTECTION ACT
Md. Comm. Code § 14-3501, *et seq*.
(On Behalf of Maryland Plaintiffs and the Maryland Subclass)

273. Plaintiffs restate and reallege the preceding paragraphs as if fully set forth herein.

274. Maryland Plaintiffs bring this claim on behalf of themselves and the Maryland Subclass.

275. Under Md. Comm. Code § 14-3503(a), "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns 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 Personal Information owned or licensed and the nature and size of the business and its operations."

276. MedStar is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

277. Plaintiffs and Class Members are "individuals" and "customers" as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

278. Plaintiffs' and Class Members' PII and PHI includes Personal Information as covered under Md. Comm. Code § 14-3501(d).

279. MedStar did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

280. The Data Breach was a "breach of the security of a system" as defined by Md. Comm. Code § 14-3504(1). Under Md. Comm. Code § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

281. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that misuse of the individual's Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security

system, the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system."

282. Because MedStar discovered a security breach and had notice of a security breach, MedStar had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

283. By failing to disclose the Data Breach in a timely and accurate manner, MedStar violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

284. As a direct and proximate result of MedStar's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiffs and Class Members suffered damages, as described above.

285. Pursuant to Md. Comm. Code § 14-3508, MedStar's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101 et seq. and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

286. Plaintiffs and Class Members seek relief under Md. Comm. Code §13-408, including actual damages and attorney's fees.

COUNT V
MARYLAND CONSUMER PROTECTION ACT
Md. Code Ann., Com. Law § 13-301, *et seq.*
(On Behalf of Maryland Plaintiffs and the Maryland Subclass)

287. Maryland Plaintiffs incorporates the foregoing allegations as though fully set forth herein.

288. Maryland Plaintiffs bring this claim on behalf of themselves and the Maryland Subclass.

289. MedStar is a person as defined by Md. Code Comm. Law § 13-101(h).

290. MedStar's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Code Comm. Law § 13-101(i) and § 13-303.

291. Class Members are "consumers" as defined by Md. Code Comm. Law § 13-101(c).

292. MedStar advertises, offers, or sell "consumer goods" or "consumer services" as defined by Md. Code Comm. Law § 13-101(d).

293. MedStar advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

294. MedStar engaged in unfair and deceptive trade practices, in violation of Md. Code, Com. Law § 13-301, including:

a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

b. Representing that consumer goods or services have a characteristic that they do not have;

c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;

d. Failing to state a material fact where the failure deceives or tends to deceive;

e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

f. Deception, fraud, false pretense, false premises, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale

lease or rental.

295. MedStar engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services in violation of Md. Code, Comm. Law § 13-303, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Comm. Law § 14-3503, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII and PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Comm. Law § 14-3503;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII and PHI; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Com. Law § 14-3503.

296. MedStar's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MedStar's data security and ability to protect the confidentiality of consumers' PII and PHI. MedStar's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

297. MedStar intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

298. Had MedStar disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, MedStar would have been unable to continue in business, and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, MedStar received, maintained, and compiled Plaintiffs' and Class Members' PII and PHI as part of the services MedStar provided and for which Plaintiffs and Class Members paid without advising Plaintiffs and Class Members that MedStar's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' PII and PHI. Accordingly, Plaintiffs and the Class Members acted reasonably in relying on MedStar's misrepresentations and omissions, the truth of which they could not have discovered.

299. MedStar acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Class Members' rights. MedStar's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

300. As a direct and proximate result of MedStar's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with MedStar as they would not have paid MedStar for goods and services or would have paid less for such goods and services but for MedStar's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII and PHI; and an increased, imminent risk of fraud and identity theft.

301. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT VI
DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT
D.C. Code § 28-3904, *et seq.*
(On Behalf of Plaintiff Bryant and the Washington D.C. Subclass)

302. Plaintiff Bryant ("Plaintiff" for the purposes of this Count) restates and realleges the preceding paragraphs as if fully set forth herein.

303. Plaintiff brings this claim on behalf of himself and the Washington D.C. Subclass.

304. MedStar is a "person" as defined by D.C. Code § 28-3901(a)(1).

305. MedStar is a "merchant" as defined by D.C. Code § 28-3901(a)(3).

306. Plaintiff and Class Members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

307. MedStar advertised, offered, or sold goods or services in the District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of the District of Columbia.

308. MedStar engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, grade, style, or model, when they are of another;

c. Misrepresenting a material fact that has a tendency to mislead;

d. Failing to state a material fact where the failure is misleading;

e. Advertising or offering goods or services without the intent to sell them as advertised or offered;

f. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

g. MedStar's unfair, unlawful, and deceptive trade practices include:

h. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

i. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures

following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

j. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

k. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII and PHI, including by implementing and maintaining reasonable security measures;

l. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII and PHI, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45;

m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII and PHI; and

n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45.

309. MedStar's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MedStar's data security and ability to protect the confidentiality of consumers' PII and PHI.

310. MedStar intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

311. The above unfair and deceptive practices and acts by MedStar were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

312. MedStar acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiff's and Class Members' rights. MedStar's past data breaches and breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

313. As a direct and proximate result of MedStar's unfair, unlawful, and deceptive trade practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with MedStar as they would not have paid MedStar for goods and services or would have paid less for such goods and services but for MedStar's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII and PHI; and an increased, imminent risk of fraud and identity theft.

314. Plaintiff and Washington D.C. Subclass Members seek all monetary and nonmonetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, attorneys' fees and costs, the greater of treble damages or $1,500 per violation, and any other relief that the Court deems proper.

COUNT VII
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

315. 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.

316. An actual controversy has arisen in the wake of the MedStar Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether MedStar is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs allege that MedStar's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and PHI and remain at imminent risk that further compromises of their PII and PHI will occur in the future.

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

318. MedStar continues to owe a legal duty to secure consumers' PII and PHI and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

319. MedStar continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

320. The Court also should issue corresponding prospective injunctive relief requiring MedStar to employ adequate security protocols consistent with law and industry standards to protect consumers' PII and PHI.

321. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at MedStar. The risk of another such breach is real, immediate, and substantial. If another breach at MedStar occurs,

Plaintiffs 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.

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

323. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at MedStar, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the class, respectfully request that the Court enter judgment in Plaintiffs' favor and against Defendant as follows:

A. Certifying the Class and Subclasses as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' counsel as Class Counsel;

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

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and

implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

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

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

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

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all claims herein so triable.

Dated: December 15, 2025.

Respectfully submitted,

/s/ Gary M. Klinger
Gary M. Klinger
MILBERG PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
gklinger@milberg.com

Jeff Ostrow
KOPELOWITZ OSTROW P.A.
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
ostrow@kolawyers.com

Danielle L. Perry*
MASON LLP
5335 Wisconsin Ave, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
dperry@masonllp.com

Plaintiffs' Interim Co-Lead Counsel

James P. Ulwick, Bar No. 00536
KRAMON & GRAHAM, P.A.
750 East Pratt Street, Suite 1100
Baltimore, Maryland 21202
Tel: 410-752-6030
julwick@kg-law.com

Plaintiffs' Liaison Counsel