CAUSE NO. 342-339562-23

SCOTT KAETHER, individually and on behalf of all others similarly situated, Plaintiff, v. METROPOLITAN AREA EMS AUTHORITY d/b/a MEDSTAR MOBILE HEALTHCARE, Defendant.	IN THE DISTRICT COURT OF TARRANT COUNTY, TEXAS _____ JUDICIAL DISTRICT

PLAINTIFF'S CLASS ACTION PETITION

Plaintiff Scott Kaether ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendant Metropolitan Area EMS Authority d/b/a MedStar Mobile Healthcare ("Medstar" or "Defendant"), an administrative governmental agency based in North Central Texas, to obtain compensatory damages, restitution, and injunctive relief for Class Members, as defined below. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack against MedStar that allowed a third party to access Defendant's computer systems, resulting in the compromise and acquisition of highly sensitive personal information (the "Data Breach") belonging to over a million current and former patients of MedStar (the "Class Members").

2. The information compromised in the Data Breach involved some of the most sensitive personal and private information available and includes names, dates of birth, contact information, and additional personally identifiable information ("PII"), as well as medical

information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") including health insurance information, medical information, and other protected health information ("PHI") (collectively the "Private Information").

3. Defendant collected and stored this Private Information on its computer network, which was compromised (and the Private Information held within acquired) during the Data Breach.

4. As a result, Plaintiff and Class Members face a heightened, imminent, and ongoing risk of identity theft and other fraudulent activity.

5. Defendant's investigation concluded that the Private Information compromised in the Data Breach included Plaintiff's and approximately 600,000 other individuals' information.[1]

6. Upon information and belief, the Data Breach was a direct result of Defendant's failure to design, implement, and monitor reasonable and adequate cyber-security procedures, policies, and protocols.

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

8. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

9. Defendant had legal obligations and duties created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

10. Defendant failed to adequately protect Plaintiff's and Class Members Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect students' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

11. Had MedStar adequately designed, implemented, and monitored its network, systems, and policies, the Data Breach would have been prevented.

12. Moreover, had MedStar informed Plaintiff that its data security was below industry standards, Plaintiff and Class Members would not have provided their Private Information to Defendant or relied on Defendant to protect that information.

13. As a result of Defendant's unreasonable and inadequate data security practices that resulted in the Data Breach, Plaintiff and Class Members are at imminent risk of identity theft and have suffered numerous actual and concrete injuries and damages, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) the loss of benefit of the bargain (price premium damages); (e) diminution of value of their Private Information; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

14. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, future costs of identity theft monitoring, and injunctive relief including improvements to Defendant's data security systems, and future annual audits.

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

PARTIES

Plaintiff Scott Kaether

17. Plaintiff Kaether is a resident and citizen of the State of Texas. Plaintiff Kaether received a notice letter regarding the Data Breach directly from Defendant, dated December 19, 2022. The letter stated that unauthorized actors gained access to files on Defendant's network and systems, which included Plaintiff's Private Information. The compromised files contained Plaintiff's name, date of birth, contact information, and information related to the medical care that Plaintiff received. Defendant obtained all of this Private Information from Plaintiff as a regular part of its business operations.

Defendant Medstar

18. Defendant Medstar is a Texas-based administrative governmental agency, with its principal place of business located at 2900 Alta Mere Drive, Fort Worth, Texas 76116.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action because the contract between Plaintiff and Defendant was established in Fort Worth (Tarrant County), Texas. Plaintiff has been damaged in a sum within the jurisdictional limits of this Court. Pursuant to Texas Rule of Civil Procedure 47, Plaintiff seeks monetary relief over $1,000,000.00. Plaintiff reserves the right to amend his petition during and/or after the discovery process. Due to the complexity of the case, discovery should be conducted pursuant to a discovery control plan under Level 3. *See* Texas Rule of Civil Procedure 190.4.

20. This Court has personal jurisdiction over Defendant because it is a resident of the State of Texas.

21. Venue is proper in this County under Tex. Civ. Prac. & Rem. Code § 15.002 because a substantial part of the events or omissions giving rise to the claim occurred in this County.

22. Upon information and belief, each of Plaintiff's individual damages are less than $75,000.

23. Upon information and belief, at least two-thirds of the Class (defined *infra*) are residents of Texas.

DEFENDANT'S BUSINESS

24. Defendant is an "administrative governmental agency" that operates in approximately fifteen North Central Texas cities and provides "Emergency Medical Services" and "advanced clinical care" to its customers.[2]

[2] https://www.medstar911.org/

25. In the ordinary course of receiving medical services from Defendant, each patient must provide (as Plaintiff did) Defendant MedStar with sensitive, personal, and private information which is then stored on MedStar's systems, including:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Demographic information;
- Information relating to the individual's dental and medical history; and,
- Insurance information and coverage.

26. Defendant also creates and stores medical records and other protected health information for its patients, including records of treatments and diagnoses on its network and computer systems.

27. As a condition of providing healthcare services to its patients, MedStar requires that each patient sign a form titled "General Medical Records Release and Authorization For Use Or Disclosure Of Protected Health Information".[3]

28. Moreover, Defendant's Notice of Privacy Practices informs patients that "[w]e are required by law to maintain the privacy of your health information, and to give you this Notice of our legal duties, our privacy practices and your rights. We are required to follow the terms of our most current Notice. When we disclose information to other persons and companies to perform services for us, we will require them to protect your privacy."[4]

[3] https://www.medstarhealth.org/-/media/project/mho/medstar/pdf/hipaa-authorization-form.pdf
[4] https://www.medstarhealth.org/-/media/project/mho/medstar/patient-privacy-policy-pdf/npp_english_2017.pdf

29. At all times, Plaintiff and Class Members relied on MedStar to protect and safeguard the Private Information through adequate data security systems, protocols, and policies. Plaintiff and Class Members further relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

30. In receiving the Private Information as part of its services, Defendant assented, promised, and undertook legal duties to safeguard and protect the Private Information entrusted to it by Plaintiff and Class Members, in compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA"), and industry standards.

31. Defendant was at all times fully aware of its obligation to protect the Private Information of its patients. Defendant was also aware of the significant damages to its patients that would result from any failures to meet its data security obligations.

THE DATA BREACH

32. On or about December 19, 2022, Defendant began sending Plaintiff and other victims of the Data Breach an untitled letter (the "Notice Letter"), informing them, in relevant part, that:

> [W]e are writing to inform you that we recently suffered a cyberattack affecting portions of protected health information for individuals we have served, which may have included your information. On October 20, 2022, we experienced issues with our network systems. We promptly investigated and determined that a third party had accessed our network. MedStar is providing this notice to give you more information on what happened and what we are doing in response.
>
> . . .

> An unauthorized third party gained access to a restricted location in MedStar's computer network that contained a number of files, including those with personal health information.[5]

33. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, whether Defendant's system is still unsecured, why it took approximately two months to inform impacted individuals after Defendant first detected the Data Breach, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

34. Medstar further admitted that the compromised files included the following customer information: "full name, date of birth, contact information, and information related to medical care provided." [6]

35. MedStar's Notice Letter claims it "promptly investigated" the Data Breach. However, MedStar nonetheless did not submit its required data breach occurrence report to the U.S. Department of Health and Human Services ("HHS") until December 19, 2022, *sixty days* after MedStar detected the Data Breach.[7]

36. The HHS requires that "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[8] Further, if "the number of individuals affected by a breach is uncertain at the time of submission,

---

[5] Ex. A.
[6] Ex. A.
[7] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[8] https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed September 13, 2022) (emphasis added).

the covered entity should provide an estimate," and later provide an addendum or correction to HSS.[9]

37. The State of Texas also specifically requires that any business that experiences a data breach "notify the attorney general of that breach not later than the 60th day after the date on which the person determines that the breach occurred if the breach involves at least 250 [Texas] residents," Tex. Bus. & Com. Code Ann. § 521.053.

38. However, MedStar did not submit a report on the Data Breach to the Office of the Texas Attorney General until January 4, 2023 (seventy-six days after MedStar detected the Data Breach).[10]

39. The State of Texas also requires that any "person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Tex. Bus. & Com. Code Ann. § 521.053(b). In fact, "breach of a security system" is defined as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information." Tex. Bus. & Com. Code Ann. § 521.053(a).

40. Because MedStar issued the data breach notification disclosure as required by Tex. Bus. & Com. Code. Ann. § 521.053, following the investigation, MedStar must have concluded that Plaintiff's and Class Members' "sensitive personal information was, or is reasonably believed to have been acquired by an unauthorized person." Tex. Bus. & Com. Code Ann. § 521.053.

[9] *Id.*
[10] https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage

Furthermore, this is consistent with the language in the Notice Letter that the data was not only accessed but also acquired –*i.e.,* stolen by the threat actors.

41. On or about October 20, 2022, MedStar knew that the Data Breach resulted in the access to and theft of patient files and that, as a result of this incident, the Private Information that was compromised and acquired by a threat actor included names, dates of birth, contact information, and medical information.

42. Upon information and belief, the Private Information contained in the files accessed and acquired by hackers was not encrypted or inadequately encrypted, as the threat actors were able to acquire and steal Plaintiff's and Class Members' Private Information.

43. In its Notice letter, Defendant acknowledged both the seriousness of the event and the increased risk to Plaintiff and Class Members with respect to the misuse of their personal information and identity theft and fraud. In the "What You Can Do" section of the Notice Letter, Defendant specifically advised, instructed, and warned Plaintiff to "remain vigilant" against incidents of identity theft and fraud and to monitor your credit reports for suspicious activity.[11]

44. Defendant's misconduct is exasperated by its feeble attempts at remedying Plaintiff and Class Members. Besides lip service regarding what class members *may* do to protect themselves, Defendant did nothing to help the impacted persons' injuries, including the impacted persons' need to monitor their financial accounts for credit fraud or identity theft.

45. In fact, Defendant did not offer to cover the payment for such a service for *any amount of time*, leaving Plaintiff and Class Members solely to their own accord for remedying the harms resulting from the Data Breach.

[11] Ex. A.

46. This is wholly inadequate to compensate Plaintiff and Class Members. Victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, which they are forced to pay for on their own despite having no culpability in the Data Breach making the monitoring necessary. Moreover, it entirely fails to provide compensation, let alone sufficient compensation, for the unauthorized release and disclosure of Plaintiff's and Class Members' PII .

Healthcare Data Breaches

47. Healthcare companies are well recognized targets for hackers and data thieves due to the volume and sensitivity of the Private Information they collect and maintain.

48. Therefore, Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry, prior to Defendant's Data Breach, and Defendant's failures to adequately design, implement and monitor systems to protect the Private Information.

49. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[12] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[13] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[14]

[12] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[13] *Id*.
[14] *Id*.

50. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in 2019 alone.[15]

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

52. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[16]

53. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including MedStar. Moreover, it was well aware of not only the risk that it would be targeted by cybercriminals but also of the severe and persistent harm that would result to its patients if it failed to protect against future

[15] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited on March 10, 2022).
[16] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware (last visited Sep. 13, 2022).

attacks. Upon information and belief, the threat actors specifically targeted MedStar with the criminal intent to acquire and steal private and confidential data for subsequent sale on the Dark Web and to commit future identity theft crimes.

Defendant Failed to Comply with FTC Guidelines

54. In light of the known risk of malware and similar data security threats, the Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

55. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

56. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

[17] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sep. 13, 2022).
[18] *Id*.

on the network; and verify that third-party service providers have implemented reasonable security measures.

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

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

59. Defendant failed to properly implement at least one or all of these basic data security practices.

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

Defendant Failed to Comply with Industry Standards

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

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

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

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

65. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and, upon information and belief, Defendant failed to comply with at least one - or all – of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant's Conduct Violated HIPAA

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

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

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

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

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

70. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

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

security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[19]

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

DEFENDANT'S DATA BREACH

72. The root cause and mechanism of the Data Breach is within the exclusive knowledge and control of Defendant and is unavailable to Plaintiff absent discovery. However, upon information and belief, the malware attack was successful because Defendant's computer network either needed security upgrading, the company lacked inadequate procedures for handling emails containing ransomware or other malignant computer code, or the company inadequately trained employees who opened files containing the ransomware virus. Defendant's unlawful conduct likely includes, but is not limited to, one or more of the following acts and/or omissions:

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

b. Failing to adequately protect patients' Private Information;

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

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

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

[19] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4.

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

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

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

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

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

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

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

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process

to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

n. Failing to notify Plaintiff of the Data Breach within 60 days after originally determining that a breach had occurred in violation of Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA"), Texas Bus. & Com. Code § 521.002 and 521.053 (2007); as amended (2019), and Texas Bus. & Com. Code § 17.46.

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity; and,

q. Otherwise failing to take reasonable steps to safeguard and protect the Private Information.

73. Accordingly, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information, and, as outlined below, Plaintiff and Class Members now face the materialized and increased risk of fraud and identity theft.

COMMON INJURIES & DAMAGES

74. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) the loss of

benefit of the bargain (price premium damages); (e) diminution of value of their Private Information; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

The Data Breached Caused an Increased Risk of Identity Theft To Plaintiff and Class Members.

75. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

76. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

77. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

78. The Private Information of consumers remains of high value to criminals, as evidenced by the prices offered through the dark web. Numerous sources cite dark web pricing for

stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[20]

79. In addition, criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

80. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[22] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[23] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

81. 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.[24] The digital character of PII 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

---

[20] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[21] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

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

[23] *Id*.

[24] *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

streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[25] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[26]

82. 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."[27]

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

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

84. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant's Notice instructs them, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.[28]

---

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

[26] *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

[27] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Sep. 13, 2022).

[28] Ex. A.

85. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such changing passwords, resecuring their own computer networks, and monitoring credit reports for unauthorized activity, which may take years to discover and detect.

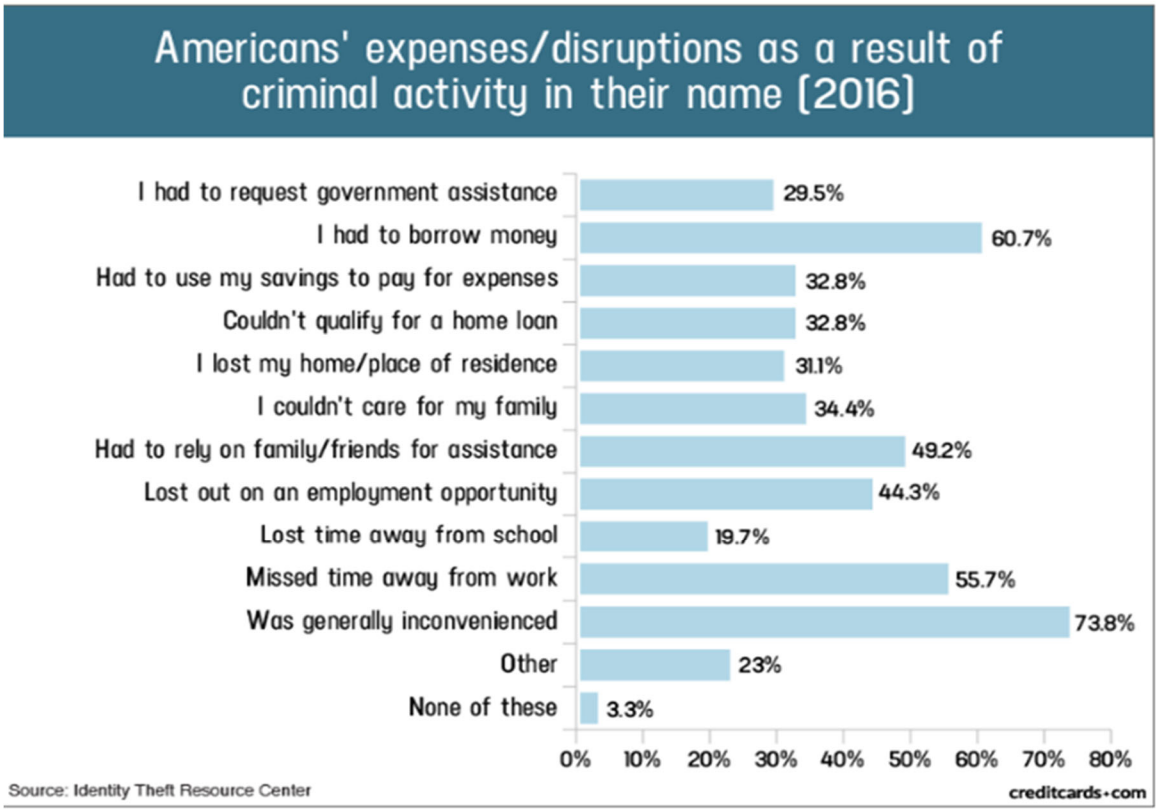
86. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[29]

87. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[30]

88. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[31]

---

[29] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[30] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[31] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Sep 13, 2022).



89. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[32]

90. 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 one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to

[32] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[33]

Diminution of Value of the Private Information

91. PII/PHI is a valuable property right.[34] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

92. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

93. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[35]

94. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data was selling on the dark web for $50 and up.[36]

---

[33] *See* https://www.identitytheft.gov/Steps (last visited Sep. 13, 2022).
[34] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[35] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).
[36] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited Sep 13, 2022).

95. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[37] In fact, the data marketplace is so sophisticated that consumers 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.[38, 39] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[40]

96. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its unauthorized release onto the Dark Web, where it is now available and holds significant value for the threat actors. However, 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 been lost, thereby causing additional loss of value.

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

97. Given the type of targeted attack, sophisticated criminal activity, and the type of PII in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

---

[37] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[38] https://datacoup.com/
[39] https://digi.me/what-is-digime/
[40] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

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

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

See GAO Report, at p. 29.

99. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

100. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[41] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as name, date of birth, and medical information).

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

[41] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

102. Defendant's misconduct is exasperated by its feeble attempts at remedying Plaintiff and Class Members To date, Defendant has offered impacted persons' *zero months* of identity monitoring services. This entirely fails to provide compensation to Plaintiff and Class Members, let alone sufficient compensation, for the unauthorized release and disclosure of Plaintiff's and Class Members' PII .

103. Victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, which Plaintiff and Class Members are forced to pay for on their own despite having no culpability in the Data Breach making the monitoring necessary.

104. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of Benefit of the Bargain

105. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for services under certain terms, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying, or being paid less, for services and data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFF SCOTT KAETHER'S EXPERIENCE

106. Plaintiff Kaether was a patient at MedStar, in or about 2017. As a condition to receive medical services at MedStar, Plaintiff Kaether was required to (and did) provide his Private Information to Defendant, which was then entered into Defendant's systems and maintained on its network.

107. Upon information and belief, during the course of his healthcare visits and as a condition of receiving services from MedStar, Plaintiff Kaether was presented with standard medical forms to complete prior to his treatment that requested his Private Information, including MedStar's HIPAA and privacy disclosure forms.

108. Plaintiff Kaether greatly values his privacy and the confidentiality of his Private Information, especially when submitting information related to health care providers. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of his Private Information -- *e. g,* Plaintiff stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents. Moreover, he diligently selects unique usernames and passwords on his various accounts; and he has not knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

109. Plaintiff Kaether received a Notice Letter concerning the Data Breach directly from Defendant, dated December 19, 2022. The letter stated that unauthorized actors gained access to and acquired files on Defendant's network, which included Plaintiff's Private Information. The compromised files contained his name, date of birth, contact information, and medical information that Defendant obtained in connection with its business operations.

110. The Notice Letter Plaintiff received also advised him to "remain vigilant" against incidents of identity theft and fraud by reviewing your account information and credit reports for suspicious activity.

111. However, to date, Defendant has not offered to cover *any amount* of identity monitoring services for Plaintiff.

112. In recognition of the present, immediate, and substantial increased risk of harm that Plaintiff Kaether faces, the cost of future identity theft protection—including five years, at the minimum, at retail cost (approximately $200 a year)—is reasonable and necessary.

113. Since learning of the Data Breach, Plaintiff Kaether has heeded Defendant's advice and warnings and spent significant time in response to the Data Breach, including changing his passwords and resecuring his own computer.

114. Plaintiff Kaether plans on taking additional time-consuming but necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial accounts for unauthorized activity.

115. As a result of the Data Breach, Plaintiff Kaether is now at a present, imminent and a continued future increased risk of identity theft, and he has suffered actual injury and damages from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) loss of benefit of the bargain; (c) loss of time mitigating the risks of identity theft, fraud, and misuse of his Private Information; (d) the reasonable and necessary future costs of identity theft monitoring; and (e) invasion of privacy.

116. The Data Breach has caused Plaintiff Kaether to suffer fear, anxiety, and stress, which has been compounded by the fact that MedStar has not been forthright about the cause and full scope of the Private Information compromised in the Data Breach.

117. As a result of the Data Breach, Plaintiff Kaether anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

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

CLASS ACTION ALLEGATIONS

119. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated.

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

> All persons whose Private Information was compromised as a result of the October 2022 Data Breach, for which MedStar provided notice on or about December 19, 2022 (the "Class").

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

122. Plaintiff hereby reserves the right to amend or modify the Class's definition with greater specificity or division or add a Subclass, after having had an opportunity to conduct discovery.

123. The proposed Class meets the criteria for certification under Rule 42(a), (b)(2), and (b)(3).

124. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiff at this time, but

MedStar has reported to the Department of Human Health and Services that the number of impacted individuals is at least 612,000.[42]

125. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

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

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

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

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

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

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

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

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

[42] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was negligent *per se*;

l. Whether Defendant's statements and/or course of dealing created an implied contract with Plaintiff to protect and safeguard their Private Information;

m. Whether Defendant's acts, inactions, and practices complained of herein amount to public disclosure of private facts under the law;

n. Whether Defendant was unjustly enriched;

o. Whether Defendant failed to provide timely and/or adequate notice of the Data Breach's occurrence; and,

p. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

126. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

127. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

128. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

130. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

131. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

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

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

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

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

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

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

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

CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

133. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

134. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

135. By collecting and storing this data in MedStar's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to design, implement, and monitor systems, policies, and processes

by which it could reasonably prevent and detect a breach of their security systems in a reasonably expeditious period of time.

136. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

137. Defendant owed a duty of care to safeguard the Private Information due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to so safeguard the Private Information.

138. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between MedStar and its patients, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, Tex. Bus. & Com. Code Ann. § 521.052, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

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

140. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .

practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

141. Defendant also had a duty under Tex. Bus. & Com. Code Ann. § 521.052(a) "to implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by [MedStar] in the regular course of business."

142. Defendant also had a duty under Tex. Bus. & Com. Code Ann. § 521.052(b) to destroy any Private Information that was no longer necessary for it to maintain.

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

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

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
b. Failing to adequately monitor the security of their networks and systems;
c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
d. Allowing unauthorized access to Class Members' Private Information;
e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

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

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

145. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

146. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

147. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

148. The imposition of a duty of care on Defendant to safeguard the Private Information it maintained is appropriate because any social utility of Defendant's conduct—to which little, if any, exists——is outweighed by the injuries suffered by Plaintiff and Class Members as a result of the Data Breach.

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

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

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

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

152. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

153. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to destroy any Private Information that it was no longer required to maintain.

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

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

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

157. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, the FTC Act, Texas statutes, and were consistent with industry standards.

158. Plaintiff 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.

159. Plaintiff 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.

160. Plaintiff 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.

161. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

162. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information or to destroy it once it was no longer necessary to retain the Private Information.

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

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

165. Plaintiff 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.

THIRD COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

166. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

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

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

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

170. Defendant also had a duty under Tex. Bus. & Com. Code Ann. § 521.052(a) "to implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by [MedStar] in the regular course of business."

171. Defendant also had a duty under Tex. Bus. & Com. Code Ann. § 521.052(b) to destroy any Private Information that was no longer necessary for it to maintain.

172. Defendant breached its duties to Plaintiff and Class Members under the FTC Act, HIPAA, and Tex. Bus. & Com. Code Ann. § 521.052, *et seq.,* by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

173. The injuries to Plaintiff and Class Members resulting from the Data breach were directly and indirectly caused by Defendant's violation of the statutes described herein.

174. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act, HIPAA, and Texas statutes were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

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

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

177. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

FOURTH COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

179. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

180. In light of the special relationship between MedStar and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, (1) to act primarily for Plaintiff and Class Members, (2) for the safeguarding of their Private Information; (3) to timely notify Plaintiff and Class Members of a Data Breach's occurence

and disclosure; and (4) to maintain complete and accurate records of what information (and where) Defendant did and does store.

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

182. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members because of the high degree of trust and confidence inherent to the nature of the relationship between Plaintiff and Class Members on the one hand and Defendant on the other, including with respect to their Private Information.

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

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

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

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

187. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating

the materialized risk and imminent threat of identity theft risk; (d) the loss of benefit of the bargain (price premium damages); (e) diminution of value of their PII; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

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

FIFTH COUNT
PUBLIC DISCLOSURE OF PRIVATE FACTS
(On Behalf of Plaintiff and the Class)

189. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

190. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

191. As a result of Defendant's conduct, publicity was given to Plaintiff's and Class Members' Private Information, which necessarily includes matters concerning their private life such as Private Information.

192. A reasonable person of ordinary sensibilities would consider the publication of Plaintiff's and Class Members' Private Information to be highly offensive.

193. Plaintiff's and Class Members' Private Information is not of legitimate public concern and should remain private.

194. As such, Defendant's conduct, as alleged above, resulted in a public disclosure of private facts, for which it is liable.

SIXTH COUNT
UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Class)

195. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

196. This count is pleaded in the alternative to the Breach of Implied Contract count above.

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

198. As such, a portion of the payments made by or on behalf of Plaintiff 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.

199. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and/or services from Defendant and/or its agents, and in so doing, provided Defendant with their Private Information based on the understanding that the benefits derived therefrom would, in part, be used to fund adequate data security. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

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

201. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information and instead directed those funds to its own profit. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to

increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

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

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

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

205. Defendant obtained a benefit from Plaintiff and Class Members by fraud and/or the taking of an undue advantage, in that it misrepresented and omitted material information concerning its data security practices when Plaintiff and Class Members relied upon it to safeguard their Private Information against foreseeable risks.

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

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

208. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and

imminent threat of identity theft risk; (d) the loss of benefit of the bargain (price premium damages); (e) diminution of value of their PII; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

209. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injuries and/or harms.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

1. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
2. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
3. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
4. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;
5. Prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;
6. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

7. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
8. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
9. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
10. Requiring Defendant to conduct regular database scanning and securing checks;
11. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
12. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
13. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing

employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

14. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

15. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

16. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

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

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

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

h) For an award of punitive damages, as allowable by law;

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

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

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

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: 01/13/ 2023

Respectfully Submitted,

/s/ *Joe Kendall*

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000
214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

GARY M. KLINGER*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

**pro hac vice forthcoming*

Attorneys for Plaintiff and the Class