Exhibit A3

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
BALTIMORE DIVISION

ANNIE SLATON, individually and on behalf of all others similarly situated, Plaintiff, v. MEDSTAR HEALTH, INC. Serve: Registered Agent The Corporation Trust Incorporated 2405 York Road Suite 201 Lutherville Timonium, MD 21093 Defendant.	CASE NO.: **CLASS ACTION COMPLAINT** (1) Negligence; (2) Breach of Implied Contract; (3) Unjust Enrichment/Quasi-Contract; (4) Violation Of DC Code § 28-3905: Unfair and Deceptive Trade Practices; (5) Violation Of the DC Data Breach Notification Statute; (6) Breach of Confidence; (7) Injunctive/Declaratory Relief **DEMAND FOR JURY TRIAL**

Plaintiff Annie Slaton ("Plaintiff"), individually and on behalf of all others similarly situated ("Class members"), alleges against MedStar Health, Inc. ("MedStar" or "Defendant"), upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, the following:

1. Plaintiff brings this Class Action Complaint against Defendant for failing to exercise reasonable care in securing and safeguarding Plaintiff's and Class members' sensitive personal data, including, but not limited to, names, dates of birth, addresses, dates of treatment, health insurance information, and provider information (collectively, "Private Information").

2. Defendant MedStar is a private, non-profit corporation headquartered in Columbia, Maryland.

3. On March 6, 2024, MedStar completed a forensic audit of its computer systems and concluded that an unauthorized party had gained intermittent access between January 25, 2023, and October 18, 2023 (the "Data Breach"). Confidential patient information was contained

in many of the emails and files accessed by this unauthorized party. As a result, the Private Information of thousands of individuals was compromised.[1]

4. Plaintiff did not receive breach notification letters until May of 2024. Defendant's failure to timely identify the Data Breach and warn Plaintiff and Class members left them particularly vulnerable.

5. Defendant's security failures enabled the hackers to steal the Private Information of Plaintiff and members of the Class (defined below). These failures put Plaintiff's and Class members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiff and Class members associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including, as appropriate, reviewing records for fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach.

6. The Data Breach was caused and enabled by Defendant's violation of their obligations to abide by best practices, industry standards, and federal and state laws concerning the security of individuals' Private Information. Defendant knew or should have known that their failure to take reasonable security measures— which could have prevented or mitigated the Data Breach that occurred— left Plaintiff's and Class members' Private Information vulnerable to identity theft, financial loss, and other associated harms.

7. Accordingly, Plaintiff asserts claims for negligence, breach of implied contract,

[1] https://www.medstarhealth.org/notice-of-data-incident (last visited May 22, 2024)

unjust enrichment/quasi-contract, violation of DC Code § 28-3905, violation of the DC Data Breach Notification Statute, and breach of confidence.

8. Plaintiff also seeks injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

PARTIES

A. PLAINTIFF ANNIE SLATON

9. Plaintiff Annie Slaton is a resident and citizen of the District of Columbia, residing at 600 Barnes Street NE Apt 425, Washington D.C., 20019. Plaintiff brings this action in her individual capacity and on behalf of all others similarly situated.

10. Plaintiff is a current patient of Defendant. She has three doctors at MedStar that she sees approximately three times a year. Her last appointment was in April of 2024.

11. In the regular course of business for receiving medical services, MedStar collected, stored, and utilized Plaintiff's Private Information.

12. In storing Plaintiff's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendants, however, did not implement proper, industry-standard safeguards to protect Plaintiff's Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

13. Shortly after May 3, 2024, Plaintiff received a notification letter from MedStar stating that her Private Information was compromised by cybercriminals.

14. Plaintiff and Class members have faced and will continue to face a certainly impending and substantial risk of future harms because of Defendant's ineffective data security measures, as further set forth herein.

15. Plaintiff Slaton greatly values her privacy and would not have chosen to disclose her Private Information to Defendant if she had known it would negligently maintain her Private Information as it did.

B. DEFENDANT MEDSTAR HEALTH, INC.

27. Defendant MedStar Health, Inc is a Maryland registered non-profit corporation with its principal place of business located on the 6th Floor of 10980 Grantchester Way, Columbia, Maryland 21044.

28. MedStar is a healthcare organization operating a number of hospitals and medical facilities in the Washington, D.C., Maryland, and Virginia areas.

JURISDICTION AND VENUE

34. The Court has subject matter and diversity jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA") because a) this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, b) there are more than 100 members in the proposed class, and c) at least one member of the Class is a citizen of a different state than Defendant, which establishes minimal diversity.

33. The Court has general personal jurisdiction over Defendant MedStar Health, Inc. because Defendant is headquartered in this District; because it operates and conducts substantial business in Maryland and this District, and because the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from Maryland and this District.

35. Venue is proper in this District under 28 U.S.C. §1391(b) because MedStar operates and is headquartered in this District; a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District; and Defendant has harmed Class members residing in this District.

FACTUAL ALLEGATIONS

36. Plaintiff and Class Members are current and former patients at MedStar facilities.

37. MedStar requires its patients, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

37. As a condition of obtaining medical services at MedStar, Plaintiff and Class Members were thus required to entrust Defendant with highly sensitive Private Information.

38. The information held by Defendant in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

39. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the Private Information collected from them as a condition of obtaining treatment at MedStar would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain the information.

40. Indeed, MedStar's Privacy Policy provides that: "MedStar Health is committed to the protection of your medical information. In our mission to serve our patients, it is our vision to be the Trusted Leader in Caring for People and Advancing Health."[2]

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

44. On or around May 5, 2024, MedStar issued Notice Letters to its patients, including Plaintiff and Class members, alerting them that their sensitive Private Information had been exposed in a Data Breach.

45. Based on the Notice Letter sent to Plaintiff and Class members, Defendant was alerted to unusual activity indicating unauthorized access to its computer systems in March of 2024. This means that Plaintiff and Class members had no knowledge their Private Information was comprised for nearly two (2) months after Defendant first learned of the Data Breach.

[2] https://www.medstarhealth.org/patient-privacy-policy (Last visited May 22, 2024).

Moreover, Defendant took over a full year from the time of the first data breach incident to conclude its forensic audit.

46. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected individuals—delay that resulted in Plaintiff and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

47. Further, the offer contained in the Notice Letter to provide 12 months of credit monitoring is woefully inadequate. Credit monitoring only alerts individuals to the misuse of their information after it happens, which might not take place until years after the Data Breach.

48. The Data Breach occurred because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other medical providers.

49. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and Class members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data. As a result, the Private Information of Plaintiff and Class members was exfiltrated through unauthorized access by an unknown, malicious cyber hacker with the intent to fraudulently misuse it. Plaintiff and Class members have a continuing interest in ensuring that their compromised Private Information is and remains safe.

A. Defendant Failed to Comply with Industry Standards and Federal and State Law

50. As a condition of obtaining healthcare services with MedStar, Plaintiff and Class Members were required to entrust Defendant, directly or indirectly, with highly sensitive Private Information.

51. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' Private Information from disclosure.

52. Defendant had obligations created by the Health Insurance Portability and Accountability Act (42 U.S.C. § 1320d et seq.) ("HIPAA"), data breach reporting requirements, state law, 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.

53. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligation and promises to keep such information confidential and secure from unauthorized access.

54. As evidenced by Defendant's failure to comply with the legal obligations established by HIPAA and state law, Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information.

55. Defendant's failure to provide adequate security measures to safeguard Plaintiff's and Class members' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to patients' Private Information. Cyber security professionals have consistently identified medical providers as particularly vulnerable to data breaches because of the value of the Private Information they collect and maintain.

56. The number of US data breaches surpassed 1,800 in 2021, a record high and a

sixty-eight percent increase in the number of data breaches from the previous year.[3]

57. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breaches and cyberattacks have resulted in significant harms to [individuals], including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for individuals' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).[4]

58. Defendant was also on notice that the FBI had been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[5]

59. The American Medical Association ("AMA") has also warned healthcare companies about the important of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.

60. The healthcare sector reported the second largest number of breaches among all

---

[3] Identity Theft Resource Center, *2021 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

[4] CONSUMER FIN. PROT. BUREAU, *Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information* (Aug. 11, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-04_circular_2022-08.pdf.

[5] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warnshealthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

measured sectors in 2018, with the highest rate of exposure per breach.[6] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[7] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and resulting identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[8]

61. A 2017 study conducted by HIMSS Analytics showed that email was the most likely cause of a data breach, with 78 percent of providers stating that they experienced a healthcare ransomware or malware attack in the past 12 months.

62. In the Healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as "incredible."[9]

63. As explained by the Federal Bureau of Investigation, "[p]revention is the most

---

[6] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, https://www.idtheftcenter.org/2018-data-breaches/.

[7] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

[8] *Id.*

[9] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results*, PROOFPOINT (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishingstatistics-2019-himss-survey-results

effective defense against ransomware and it is critical to take precaution for protection."[10]

64. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filers to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suit applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

[10] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

65. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[11]

66. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;

- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for

[11] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

Office [Visual Basic for Applications].[12]

67. These are basic, common sense security measures that every business, not only healthcare businesses, should take. Medstar, with its heightened standard of care, should have done even more. By adequately taking these common sense measures, Medstar could have prevented this Data Breach from occurring.

68. Charged with handling sensitive Private Information, Defendant knew, or should have known, the importance of safeguarding individuals' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiff and Class members after a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

69. Despite the abundance and availability of information regarding cybersecurity best practices for medical providers, Defendant chose to ignore them. These best practices were known, or should have been known, by Defendant, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

70. At a minimum, industry best practices should have been implemented by Defendant, including but not limited to requiring users to create strong passwords; implementing multi-layer security including firewalls and anti-malware software; encrypting data and making it unreadable without a key; updating and patching all systems with the latest security software; and better educating its patients about safe data security practices.

71. Defendant apparently did not follow these precautions because cybercriminals accessed individuals' Private Information off MedStar's network until MedStar was able to cease the unauthorized access.

---

[12] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020). https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

72. Defendant was also on notice that under the FTC Act, Defendant is prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for individuals' sensitive personal information is an "unfair practice" in violation of the FTC Act.[13]

73. Defendant is further required by the comprehensive data privacy regimes enacted by at least 13 states to protect Plaintiff's and Class members' Private Information, and further, to handle any breach of the same in accordance with applicable breach notification statutes.[14]

74. The potential for improper disclosure of Plaintiff's and Class members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

75. Moreover, Defendant's conduct violated HIPAA. HIPAA requires covered entities like MedStar to protect against reasonably anticipated threats to the security of Personal Health Information ("PHI"). Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[15]

76. 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 Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

---

[13] *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

[14] International Association of Privacy Professionals, *Delaware Governor Signs Personal Data Privacy Act* (Sep. 12, 2023), https://iapp.org/news/a/delaware-governor-signs-personal-data-privacy-act.

[15] *What is Considered Protected Health Information Under HIPAA*?, HIPPA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

77. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[16]

78. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. CRHS's security failures include, but are not limited to, the following:

- Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);
- Failing to implement 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 in violation of 45 C.F.R. §164.312(a)(1);
- 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);
- Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);
- Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);
- Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);
- Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. §164.306(a)(94);

[16] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

- Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

- Failing to effectively train all members of its workforce (including agents and independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

- Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

B. Defendant Exposed the Class to Identity Theft, Financial Loss, and Other Harms

79. Plaintiff and Class members have been injured by the disclosure of their Private Information in the Data Breach.

80. The fact that Plaintiff's and Class members' Private Information was stolen means that Class members' information is likely for sale by cybercriminals and will be misused in additional instances in the future.

81. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft and financial fraud.[17] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

82. The value of Plaintiff's and Class members' Private Information on the black market is substantial. Indeed, studies confirm that the average direct financial loss for victims of

[17] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

identity theft in 2014 was $1,349.[18]

83. The FTC has also recognized that personal data is a valuable form of currency. In an FTC roundtable presentation, a former Commissioner, Pamela Jones Harbour, underscored this point:

> *Most [people] cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.*[19]

84. Recognizing the high value that individuals place on their Private Information, many companies now offer individuals an opportunity to sell this information.[20] The idea is to give individuals more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, individuals will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

85. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

86. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the breach of its systems and, ultimately, the theft of Plaintiff's and Class members' Private Information.

---

18 *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

19 *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

20 *Web's Hot New Commodity*, *supra* note 17.

87. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about an individual that can be logically associated with other information can be chained together, increasing its utility to criminals.

88. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

89. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

90. The Department of Health and Human Services Office for Civil Rights has stated:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[21]

91. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

92. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because of the value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[22] They too have promulgated similar best practices for bolstering

---

[21] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.

[22] *See, e.g.*, *10 Best Practices For Healthcare Security*, INFOSEC, https://resources.infosecinstitute.com/topics/healthcare-information-security/#gref.

cybersecurity and protecting against the unauthorized disclosure of Private Information.

93. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Medstar chose to ignore them. These best practices were known, or should have been known, by Medstar, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

C. Plaintiff and Class Members Suffered Damages from the Data Breach

94. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

95. The ramifications of Defendant's failure to keep the Class's Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Victims of data breaches are more likely to become victims of identity fraud.[23]

96. In addition to its obligations under state and federal laws and regulations, Defendant owed a common law duty to Plaintiff and Class members to protect the Private Information they entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

97. Defendant further owed and breached its duty to Plaintiff and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

98. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiff's and Class

[23] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

members' Private Information as detailed above, and Plaintiff and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

99. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some individuals victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

100. Plaintiff and the Class continue to face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, applications for benefits made fraudulently in their names, loans opened in their names, medical services billed in their names, government benefits fraudulently drawn in their name, and identity theft. Many Class members may already be victims of identity theft and fraud without realizing it.

101. Plaintiff and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

102. Plaintiff and Class members did not receive the full benefit of their bargain when exchanging their private personal data for Defendant's services as a medical provider. Plaintiff and Class Members should have received the privacy protections that they were guaranteed by Defendant as a part of their receiving treatment from Defendant.

103. Plaintiff and Class members were damaged in an amount at least equal to the difference in the value between the services they thought they received (which would have included adequate data security protection) and the services they actually received.

104. Plaintiff and Class members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

105. Plaintiff and the Class will continue to spend significant amounts of time to

monitor their financial accounts for misuse.

106. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Private Information and will need to monitor their credit for an indefinite duration. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet failed to properly prepare for that risk.

107. As a result of the Data Breach, Plaintiff and Class members' Private Information has diminished in value.

108. The Private Information belonging to Plaintiff and Class members is private and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed Plaintiff's and Class members' Private Information as a direct result of its inadequate security measures.

109. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

110. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

111. Defendant did not properly train its employees, particularly its information technology department, to timely identify cyber-attacks and other data security risks.

112. Had Defendant remedied the deficiencies in its data security systems and adopted

security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class members' Private Information.

113. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

114. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[24]

115. Defendant did not take any substantive measures to assist Plaintiff and Class members.

116. There may be a time lag between when harm occurs versus when it is discovered, and between when Private Information is acquired and when it is used. Furthermore, solutions like identity theft monitoring only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[25]

117. Defendant's failure to adequately protect Plaintiff's and Class members' Private Information has resulted in Plaintiff and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by

[24] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[25] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

the incident. Instead, as MedStar's notice confirms, the burden is on Plaintiff and Class members to discover possible fraudulent activity and identity theft and mitigate on their own the negative impacts arising from such fraudulent activity.

118. Plaintiff and Class members have been damaged in several other ways as well. Plaintiff and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming task. Class members have also been forced to purchase adequate credit reports, credit monitoring and other identity protection services, and/or have placed credit freezes and fraud alerts on their credit reports, while also spending significant time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and Class members also suffered a loss of the inherent value of their Private Information.

119. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

120. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

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

- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fail to undertake appropriate measures to protect the Private Information in their possession;

- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members; and

- Anxiety and distress resulting from fear of misuse of their Private Information.

121. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

116. Plaintiff brings all counts, as set forth below, individually and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a "Nationwide Class" (collectively, the "Class") and a Washington, D.C. Subclass (D.C. Subclass) defined as:

Nationwide Class

All persons who submitted their Private Information to MedStar and whose Private Information was compromised as a result of the data breach(es) discovered in or about March of 2024.

Washington, D.C. Subclass

All persons in Washington D.C. who submitted their Private Information to Medstar and whose Private Information was compromised as a result of the data

breach(es) discovered in or about March of 2024.

117. Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, patients, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

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

119. **Numerosity**—Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Class has thousands of members.

120. **Commonality and Predominance**—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, inter alia:

a. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., FTCA and HIPAA (as discussed above and below);

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

c. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

e. Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed by its patients in confidence and should be maintained;

f. Whether Defendant's conduct constitutes breach of an implied contract;

g. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;

h. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;

i. Whether Defendant was unjustly enriched by its actions; and

j. Whether Plaintiff and the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

121. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

122. **Typicality**—Federal Rule of Civil Procedure 23(a)(3). Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

123. **Adequacy of Representation**—Federal Rule of Civil Procedure 23(a)(4).

Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class she seeks to represent, she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

124. **Injunctive Relief**—Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

125. **Superiority**—Federal Rule of Civil Procedure 23(b)(3). 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 or other financial detriment suffered by Plaintiff and the Class 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 members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class 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 a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class, or in the alternative On Behalf of the D.C. Subclass)

126. Plaintiff fully incorporates by reference all the above paragraphs, as though fully

set forth herein.

127. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that Class members' Private Information was private and confidential and should be protected as private and confidential.

128. Defendant owed a duty of care not to subject Plaintiff's and Class members' Private Information to an unreasonable risk of exposure and theft because Plaintiff and Class members were foreseeable and probable victims of any inadequate security practices.

129. Defendant owed numerous duties to Plaintiff and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

130. Defendant also breached a duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information and potentially misuse it and intentionally disclose it to others without consent.

131. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should

have known about numerous well-publicized data breaches within the medical industry.

132. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' Private Information.

133. Defendant was in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

134. Defendant breached duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

135. Because Defendant knew that a breach of its systems would damage thousands of individuals, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained therein.

136. 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.

137. Defendant had numerous duties to safeguard patient PHI and Personally Identifiable Information ("PII") under HIPAA, as detailed above.

138. 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.

139. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff's and Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

140. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant includes,

but is 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 Defendant's networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

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

e. 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.

141. Through Defendant's acts and omissions described in this Complaint, including their failure to provide adequate security and its failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendant's possession or control.

142. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

143. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

144. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

145. 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 lifetime free credit monitoring to all Class members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class, or in the alternative On Behalf of the D.C. Subclass)

146. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

147. As a condition of receiving treatment, Plaintiff and Class members were required to provide Defendant with their Private Information.

148. In so doing, Plaintiff and Class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. 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 and were consistent with industry standards.

149. Defendant's contracts contain numerous references to HIPAA and assure clients of Defendant's compliance.

150. Plaintiff and Class members would not have provided and entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendants.

151. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendants.

152. Defendant breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect their Private Information and by failing to detect the Data Breach within a reasonable time.

153. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant, Plaintiffs, and Class members, Plaintiff and Class members sustained actual losses and damages as described in detail above.

154. 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 free credit monitoring to all Class members.

COUNT III
UNJUST ENRICHMENT/QUASI-CONTRACT
(On Behalf of the Nationwide Class, or in the alternative on Behalf of the D.C. Subclass)

155. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

156. Plaintiff and Class members conferred monetary benefits on Defendant when they exchanged their sensitive Private Information to receive medical care.

157. In exchange, Plaintiff and Class Members should have received the medical care that was the subject of the exchange. Plaintiff and the Class were entitled to assume their medical care included adequate data security for their Private Information.

158. Defendant knew that Plaintiff and Class members conferred benefits upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's and Class members' retained data and used Plaintiff's and Class members' Private Information for business purposes.

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

160. Defendant acquired the Private Information through inequitable means as it failed to disclose the inadequate security practices previously alleged.

161. If Plaintiff and Class members had known that Defendant would not secure their Private Information using adequate security, they would not have entrusted Defendant with their Private Information.

162. Plaintiff and Class members have no adequate remedy at law.

163. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on it.

164. Defendant should be compelled to disgorge into a common fund or constructive

trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them.

COUNT IV
VIOLATION OF DC CODE § 28-3905:
UNFAIR AND DECEPTIVE TRADE PRACTICES
(Plaintiff, individually and on behalf of the D.C. Subclass)

165. Plaintiff realleges and incorporates by reference the above allegations.

166. Plaintiff, on behalf of herself individually and on behalf of all others similarly situated, files this action pursuant to D.C. Code § 28-3905(k).

167. The District of Columbia Consumer Protection Procedures Act ("CPPA") prohibits unlawful trade practices in connection with the offer, lease, and supply of consumer goods. 28-3901(a)(6). Consumer goods include "healthcare services." 28-3901(a)(7).

168. The CPPA defines merchant as "a person, whether organized or operating for profit or for nonprofit purpose, who in the ordinary course of business does or would sell, lease (to), or transfer, either directly or indirectly, consumer goods or services, or a person who in the ordinary course of business does or would supply the goods or services which are or would be the subject matter of a trade practice." CPPA. 28-3901(a)(3). "A 'merchant' is not limited to the direct supplier of goods or services to consumers, but includes any person connected with the supply-side of a consumer transaction." *District of Columbia v. Student Aid Ctr., Inc.*, 2017 D.C. Super. LEXIS 18, *5 (September 8, 2017); *see also Hall v. S. River Restoration, Inc.*, 270 F. Supp. 3d 117, 123 (D.D.C. 2017) (citations and quotations omitted) ("[a] merchant need not be the actual seller of the goods or services complained of but must be connected with the supply side of the consumer transaction").

169. Defendant is a merchant under the CPPA because it operates facilities involved in the provision of healthcare services and/or is otherwise sufficiently connected to supplying healthcare services to consumers.

170. The CPPA defines consumer as a person who "does or would purchase, lease (as lessee), or receive consumer goods...or does or would otherwise provide the economic demand for a trade practice." 28-3901(a)(2). Plaintiff and Class members have received healthcare services and otherwise provided the economic demand for the trade practice and are therefore consumers under the CPPA.

171. Under the CPPA, it is an unlawful trade practice to:

a. represent that goods or services have a source, sponsorship, approval, certification, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have;
b. represent that goods or services are of a particular standard, quality, grade, style, or model, if, in fact, they are of another;
c. misrepresent as to a material fact which has a tendency to mislead;
d. fail to state a material fact if such failure tends to mislead; and,
e. use innuendo or ambiguity as to a material fact, which has a tendency to mislead; D.C. Code 28-3904.

172. Defendant violated the CPPA by, among other things:

a. Representing and misrepresenting, expressly and implicitly, that Defendant's privacy and security practices were sufficient to ensure the safety of Plaintiff and Class members' health information.
b. Representing and misrepresenting, expressly and implicitly, that Defendant complied with all applicable laws concerning the maintenance and protection of private health information.
c. Representing and misrepresenting that Defendant would take affirmative steps to ensure the security of Plaintiff and Class members' private information.

173. Defendant intentionally made these misrepresentations or omissions knowing it misled reasonable consumers, such as Plaintiff.

174. These misrepresentations and omissions had the capacity and tendency to mislead consumers. D.C. Code § 28-3901(c) establishes an enforceable right to truthful information from merchants about consumer goods and services that are or would be received in the District of Columbia.

175. Defendant's unfair and deceptive acts and omissions were flagrant and willful and created an imminent danger to Plaintiff and the putative class.

176. Defendant's acts and omissions are unfair in that they (1) offend public policy; (2) are immoral, unethical, oppressive, and unscrupulous; and (3) cause substantial injury to consumers.

177. Defendant's acts and omissions are also unfair in that they cause substantial injury to consumers far in excess of any conceivable benefit; and are injuries of a nature that could not have been reasonably avoided by consumers.

178. As a result of Defendant's unfair and deceptive trade practices detailed herein, Plaintiff and the Class have suffered substantial injury including, but not limited to, paying more for healthcare services than they otherwise would have had they known Defendant would not secure their Private Information; increased likelihood of fraud and misuse of personal information; spending time and resources preventing and alleviating fraud and misuse of their personal data; and expending time and resources attempting to compel Defendant to perform its legally-required duties.

179. As a result of Defendant's unfair and deceptive trade practices, Plaintiff seeks on behalf of herself and the DC Subclass:

A. An injunction against Defendant, requiring Defendant to encrypt all personal information stored on its servers, or that Defendant modify its privacy policy to accurately reflect its data security practices;

B. Additional relief to restore to the consumer money which was acquired by means of the unlawful trade practices within the District of Columbia;

C. Punitive damages;

D. $1500 per violation or treble damages, whichever is greater;

E. Reasonable Attorney's fees;

F. All other statutory relief the Court deems proper under D.C. Code § 28-3905(k)(1).

Count V
VIOLATION OF THE DC DATA BREACH NOTIFICATION STATUTE
(Plaintiff, individually and on behalf of the D.C. Subclass)

180. Each of the preceding paragraphs is incorporated by reference herein.

181. The District of Columbia Data Breach Notification Statute (D.C. Code, Loc. Bus. Aff. § 28-3851, et seq.) defines "personal information" as:

> An individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements:
>
> (II) Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account;
>
> (III) Medical information;
>
> * * *
>
> (V) Health insurance information, including a policy number, subscriber information number, or any unique identifier used by a health insurer to identify the person that permits access to an individual's health and billing information[.]

D.C. Code § 28-3851(3).

182. Pursuant to Defendant's notice to its patients, the following information of Plaintiff Slaton was breached – name, mailing address, date of birth, date(s) of service, provider name(s), and/or health insurance information.

183. Defendant was therefore required to notify Plaintiff Slaton and the DC Subclass in the "most expedient time possible" and without unreasonable delay. Defendant was further required to notify all Consumer Reporting Agencies without unreasonable delay of the breach of information of Plaintiff Slaton and the DC Subclass, which is in excess of 1000 individuals.

184. Defendants failed to provide notice of the data breach to Plaintiff Slaton and the DC Subclass in the most expedient time possible and also failed to provide notice of the breach to all required Consumer Reporting Agencies without unreasonable delay.

185. Plaintiff Slaton and the DC Subclass have suffered actual damages in that she and members of the DC Subclass have purchased and/or will need to continue to purchase credit monitoring and identity theft protection for life.

186. Plaintiff Sloan brings this cause of action on behalf of herself individually and the DC Subclass seeking all actual damages, costs of the action and reasonable attorneys' fees.

COUNT VI
BREACH OF CONFIDENCE
(On Behalf of the Nationwide Class, or in the alternative on Behalf of the D.C. Subclass)

187. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

188. Plaintiff and Class members have an interest, both equitable and legal, in the Private Information that was conveyed to and collected, stored, and maintained by Defendant and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

189. Defendant, in taking possession of this highly sensitive information, has a special relationship with Plaintiff and the Class. As a result of that special relationship, Defendant was

provided with and stored private and valuable information belonging to Plaintiff and the Class, which Defendant was required by law and industry standards to maintain in confidence.

190. Plaintiff and the Class provided such Private Information to Defendant under both the express and/or implied agreement of Defendant to limit and/or restrict completely the use and disclosure of such Private Information without Plaintiff's and Class members' consent.

191. Defendant had a common law duty to maintain the confidentiality of Plaintiff's and Class members' Private Information.

192. Defendant owed a duty to Plaintiff and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in Defendant's possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

193. As a result of the parties' relationship of trust, Defendant had possession and knowledge of the confidential Private Information of Plaintiff and Class members.

194. Plaintiff's and Class members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiff and Class members did not consent to nor authorize Defendant to release or disclose their Private Information to unknown criminal actors.

195. Defendant breached the duty of confidence it owed to Plaintiff and Class members when Plaintiff's and Class members' Private Information was disclosed to unknown criminal hackers by way of Defendant's own acts and omissions, as alleged herein.

196. Defendant knowingly breached its duties of confidence by failing to safeguard Plaintiff's and Class members' Private Information, including by, among other things: (a) mismanaging its systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information that resulted in the unauthorized access and compromise of the Private Information; (b) mishandling data security by failing to assess the sufficiency of the safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

(e) failing to evaluate and adjust its information security programs in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiff and Class members thereof; (g) failing to follow its own privacy policies and practices; (h) storing Private Information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class members' Private Information to a criminal third party.

197. But for Defendant's wrongful breach of confidence owed to Plaintiff and Class members, their privacy would not have been compromised and their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

198. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality in their Private Information; theft of their Private Information; costs associated with the detection and prevention of fraud and unauthorized use of their Private Information; costs associated with purchasing credit monitoring and identity theft protection services; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant's Data Breach – including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with the police and FBI; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of 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 Plaintiff's and Class members' data; and/or mental

anguish accompanying the loss of confidence and disclosure of their confidential Private Information.

199. Defendant breached the confidence of Plaintiff and Class members by making an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for Defendant to retain the benefits it has received at Plaintiff's and Class members' expense.

200. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VII
INJUNCTIVE / DECLARATORY RELIEF
(On Behalf of the Nationwide Class, or in the alternative on Behalf of the D.C. Subclass)

201. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

202. 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. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

203. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective duties to reasonably safeguard users' Private Information and whether Defendant are maintaining data security measures adequate to protect the Class members, including Plaintiffs, from further data breaches that compromise their Private Information.

204. Plaintiff alleges that Defendant's data-security measures remain inadequate. In addition, Plaintiff and the Class continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information and fraudulent activity against them will occur in the future.

205. Pursuant to the Court's authority under the Declaratory Judgment Act, Plaintiff

asks the Court to enter a judgment declaring, among other things, the following: (i) Defendant owes a duty to secure individuals' Private Information and to timely notify them of a data breach under the common law and various federal and state statutes; and (ii) Defendant is in breach of these legal duties by failing to employ reasonable measures to secure individuals' Private Information in its possession and control.

206. Plaintiff further asks the Court to issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect individuals' Private Information from future data breaches.

207. If an injunction is not issued, the Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendants. The risk of another such breach is real, immediate, and substantial. If another breach of Defendant occurs, the Class members will not have an adequate remedy at law because many of the resulting injuries would not be readily quantifiable and Class members will be forced to bring multiple lawsuits to rectify the same misconduct.

208. The hardship to the Class members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of Defendant, the Class members will likely be subjected to substantial hacking and phishing attempts, fraud, and other instances of the misuse of their Private Information, in addition to the damages already suffered. On the other hand, the cost to Defendant of complying with an injunction by employing better and more reasonable prospective data security measures is relatively minimal, and Defendant has pre-existing legal obligations to employ such measures.

209. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches of Defendant, thus eliminating the additional injuries that would result to the Class members and the individuals whose personal and confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an order certifying the proposed Class and appointing Plaintiff and her counsel to represent the Class;

b. For an order awarding Plaintiff and Class members actual, statutory, punitive, and/or any other form of damages provided by and pursuant to the statutes cited above;

c. For an order awarding Plaintiff and Class members restitution, disgorgement and/or other equitable relief provided by and pursuant to the statutes cited above or as the Court deems proper;

d. For an order or orders requiring Defendant to adequately remediate the Breach and its effects.

e. For an order awarding Plaintiff and Class members pre-judgment and post-judgment interest;

f. For an order awarding Plaintiff and Class members treble damages, other enhanced damages and attorneys' fees as provided for under the statutes cited above and related statutes;

g. For an order awarding Plaintiff and the Class members reasonable attorneys' fees and costs of suit, including expert witness fees;

h. For an order awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Dated: May 24, 2024

By: /s/ *Nicholas A. Migliaccio*
Nicholas A. Migliaccio
(Maryland Federal Bar No. 29077)

Jason S. Rathod
(Maryland Federal Bar No. 18424)
MIGLIACCIO & RATHOD LLP
412 H Street NE, Ste. 302,
Washington, DC, 20002
Office: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Attorneys for Plaintiff and the Proposed Class