IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

ROBERT BOWEN, individually and on behalf of all others similarly situated, Plaintiff, v. HEALTHCARE SERVICES GROUP, INC., Defendant.	Case No. **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Robert Bowen ("Plaintiff"), individually and on behalf of all others similarly situated, by and through the undersigned attorneys, brings this class action against Defendant Healthcare Services Group, Inc. ("HSG" or "Defendant") and complains and alleges upon personal knowledge as to his own actions and their counsels' investigations, and upon information and good faith belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against HSG for its failure to secure and safeguard personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Personal Information") for approximately 624,496 individuals.

2. HSG is a Bensalem, Pennsylvania-based entity that provides management, administrative, and operating expertise and services primarily to the healthcare industry, including nursing homes, retirement complexes, rehabilitation centers, and hospitals across the United States.

3. Customers or patients of HSG's customers are required to provide HSG with, or otherwise allow HSG to collect, sensitive Personal Information. By being entrusted with this sensitive information, HSG assumed a legal duty to reasonably safeguard it.

4. The data breach at issue in this litigation ("Data Breach") involved unauthorized access to HSG's network, with initial access detected on September 27, 2024, and the intrusion identified 10 days later on October 7, 2024. The breach potentially exposed the PII and PHI of 624,496 individuals.

5. According to HSG and public reports, the exposed information may include names, Social Security numbers, driver's license numbers, state identification numbers, financial account details, and other PII. The exact data compromised varies by individual, but HSG confirmed that sensitive personal and health information was potentially stolen.

6. HSG's August 25, 2025 consumer notification was posted on the Maine Attorney General's website.[1] The notice merely states that HSG is mailing letters to affected individuals and offering 12 months of credit monitoring services.

7. The consumer notification acknowledges that Plaintiff's and class members' Personal Information was unlawfully accessed by the cyber criminals, but HSG did not disclose how HSG discovered the files on its computer systems were impacted, the means and mechanism of the cyberattack, the reason for the 10-month delay in disclosing the Data Breach, how it determined that the PII/PHI had been accessed by the unauthorized actor(s), and, importantly, what specific steps it took following the Data Breach to secure its systems and prevent future cyberattacks.

8. The Data Breach was a direct result of HSG's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Personal Information from the foreseeable threat of a cyberattack.

[1] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/9a82ac2b-5379-462d-acd6-26a3b3bd0b30.html (last visited Aug. 27, 2025).

9. Plaintiff brings this class action lawsuit individually and on behalf of those similarly situated to address HSG's inadequate safeguarding of Plaintiff's and class members' Personal Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and class members.

10. Plaintiff brings claims for negligence, breach of fiduciary duty, unjust enrichment, and declaratory and injunctive relief. To remedy these violations of law, Plaintiff and class members seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to HSG's data security protocols and employee training practices); reasonable attorneys' fees, costs, and expenses incurred in bringing this action; and all other remedies this Court deems just and proper.

PARTIES

Plaintiff

Plaintiff Robert Bowen

11. Plaintiff Robert Bowen is a resident of Jasper County, Iowa and citizen of the State of Iowa.

12. Plaintiff is a former employee of HSG in Carroll, Iowa where Plaintiff was employed as a Dietary Manager for Regency Park Nursing & Rehabilitation Center of Carroll, a nursing facility that utilized HSG's services at the time of Plaintiff's employment. As a condition of his employment, Plaintiff provided PII/PHI, directly or indirectly, to HSG in connection with his job. In requesting and maintaining Plaintiff's Personal Information for its business purposes, HSG undertook a duty to act reasonably in its handling of Plaintiff's Personal Information. On information and belief, HSG did not take proper care of Plaintiff's Personal Information, leading to its exposure by cybercriminals as a direct result of its inadequate security measures.

13. Plaintiff is very careful about sharing sensitive Personal Information. Plaintiff has never knowingly transmitted unencrypted sensitive Personal Information over the internet or any other unsecured source.

14. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the breach, and time spent closely monitoring potentially compromised accounts and activity occurring with potentially compromised data. This time has been lost forever and cannot be recaptured.

15. Once Personal Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff will need to maintain these heightened measures for years.

16. Plaintiff also suffered actual injury from having Personal Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential personal information—a form of intangible property that Plaintiff entrusted to HSG, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of Plaintiff's privacy rights as a result of HSG's unauthorized disclosure of Personal Information.

17. Had Plaintiff known that HSG does not adequately protect PII/PHI, Plaintiff would not have sought employment with HSG and would not have agreed to provide HSG with PII/PHI or have it approved.

18. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy.

19. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from Personal Information being placed in the hands of unauthorized third parties and possibly criminals.

20. As a result of HSG's failure to adequately safeguard Plaintiff's information, Plaintiff has been injured. Plaintiff is also at a continued risk of harm because upon information and belief the Personal Information remains in HSG's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as HSG fails to undertake the necessary and appropriate data security measures to protect the PII and PHI in its possession.

Defendant

21. Defendant Healthcare Services Group, Inc. is a corporation formed under the laws of the Commonwealth of Pennsylvania with corporate headquarters located at 3220 Tillman Drive, Suite 300, Bensalem, Pennsylvania 19020.

JURISDICTION AND VENUE

22. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the class is a citizen of a different state than Defendant, there are more than 100 members of the class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

23. This Court has personal jurisdiction over HSG because HSG maintains its principal place of business in Pennsylvania and conducts substantial business in Pennsylvania and in this district through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, HSG resides in this district, maintains Plaintiff's and class members' Personal Information in this district, and this district is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

FACTUAL ALLEGATIONS

A. Overview of HSG Health

25. Founded in 1976, HSG is a Bensalem-based entity management, administrative, and operating expertise and services primarily to the healthcare industry, including nursing homes, retirement complexes, rehabilitation centers, and hospitals across the United States.

26. HCSG serves approximately 2,200 facilities for housekeeping services and 1,600 for dietary services, aiming to enhance operational, regulatory, and financial outcomes through efficient systems, team accountability, and quality assurance programs. The company employs around 35,700 people and operates in 48 states.

27. In the regular course of its business, HSG collects and maintains PII/PHI. As a regular part of its business, HSG requires individuals to provide personal information directly or indirectly before it provides its services. HSG also collects PII/PHI from its employees as a condition of their employment. HSG stores this information digitally.

28. HSG is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA Security Rule[2] and to report any unauthorized use or disclosure of Personal Information, including

[2] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the

incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

29. In its Privacy Policy, HSG affirms that it "respects the privacy of our users,"[3] yet HSG maintained inadequate security measures which allowed the Data Breach to occur. It then waited 10 months after discovering the Data Breach to disclose that PII/PHI had been compromised.

30. Plaintiff and class members are, or were, current or former employees, patients of customers of HSG's customers and/or received health-related or other services from HSG, or otherwise are affiliated or transacted with HSG, and entrusted HSG with their PII/PHI or otherwise had their PII/PHI entrusted to HSG.

31. Because of the highly sensitive and personal nature of the information HSG acquires and stores, Plaintiff and class members reasonably expect that HSG will, among other things: keep their Personal Information confidential; comply with healthcare industry standards related to data security and Personal Information; inform them of legal duties and comply with all federal and state laws protecting their Personal Information; only use and release their Personal Information for reasons that relate to medical care and treatment; and provide adequate notice to them if their Personal Information is disclosed without authorization.

B. HSG Is a HIPAA Covered Business Entity

32. HSG is a HIPAA covered business entity that provides healthcare services to healthcare providers and, through those providers, Plaintiff and class members. As a condition of benefiting from HSG's services, HSG requires that Plaintiff and class members provide it with (or

confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[3] https://www.hcsgcorp.com/privacy-policy/ (last visited Aug. 27, 2025).

have provided on their behalf) highly sensitive Personal Information. Due to the nature of HSG's business of providing health services, HSG would be unable to engage in its regular business activities without collecting and aggregating Personal Information that it knows and understands to be sensitive and confidential.

33. HSG is required under federal and state law to maintain the strictest confidentiality of Personal Information that it requires, receives, and collects, and HSG is further required to maintain sufficient safeguards to protect that Personal Information from being accessed by unauthorized third parties, and to report any unauthorized use or disclosure of Personal Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

34. Plaintiff and class members are or were individuals whose sensitive information was maintained by HSG, and directly or indirectly entrusted HSG with their Personal Information. Plaintiff and class members reasonably expected that HSG would safeguard their highly sensitive information and keep their Personal Information confidential.

C. The Data Breach Compromised Plaintiff's and Class Members' PII/PHI

35. According to the privacy notification provided by HSG to state attorneys' general (to be disseminated to impacted persons), HSG was subject to a cybersecurity attack beginning on or before September 27, 2024 that lasted until October 3, 2024.

36. On October 7, 2024, HSG discovered that the Data Breach may have impacted Personal Information stored in its systems.

37. HSG confirmed that these files included, but may not be limited to: names, Social Security numbers, driver's license numbers, state identification numbers, financial account details, and access credentials.

38. HSG did not publicly announce the Data Breach until 10 months later, in August 2025. The notice provides scant details of what occurred, but confirms that HSG's "investigation determined that an unauthorized actor may have accessed and copied certain files on HSG[]'s computer systems . . . ."

39. HSG's disclosures omit pertinent information including how criminals gained access to the files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, how it determined that the Personal Information had been accessed, and, of particular importance to Plaintiff and class members, what actual steps HSG took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks.

40. Based on HSG's acknowledgment that Personal Information was accessed by an unauthorized party, it is evident that unauthorized criminal actors did, in fact, access HSG's network and thus Plaintiff's and class members' Personal Information in an attack designed to acquire that sensitive, confidential, and valuable information.

41. The Personal Information contained in the files accessed by cybercriminals appears not to have been encrypted, because, if properly encrypted, the attackers would have acquired unintelligible data and would not have "accessed" Personal Information.

42. The Data Breach reportedly impacted the protected health information of 624,496 individuals.[4]

43. As a (on information and belief) HIPAA-covered business entity that collects, creates, and maintains significant volumes of personal information, the targeted attack was a foreseeable risk of which HSG was aware and knew it had a duty to guard against.

[4] Note 1, *supra*.

44. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Personal Information of Plaintiff and class members.

45. Due to HSG's inadequate security measures, Plaintiff and class members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

46. HSG had obligations created by HIPAA, contract, industry standards, and common law to Plaintiff and class members to keep their Personal Information confidential and to protect it from unauthorized access and disclosure.

47. Plaintiff and class members entrusted their Personal Information to HSG, or otherwise had that information provided to HSG, with the reasonable expectation and mutual understanding that HSG or anyone who used their Personal Information in conjunction with the healthcare services they received would comply with obligations to keep such information confidential and secure from unauthorized access after it received such information.

48. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and class members' Personal Information, HSG assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and class members' Personal Information from unauthorized disclosure.

49. Plaintiff and the class members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiff and class members would not have allowed HSG or anyone in HSG's position to receive their PII/PHI had they known that HSG would fail to implement industry standard protections for that sensitive information.

50. As a result of HSG's negligent and wrongful conduct, Plaintiff's and class members' highly confidential and sensitive Personal Information was left exposed to cybercriminals. The unencrypted Personal Information of Plaintiff and class members will end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed Personal Information for targeted marketing without the approval of Plaintiff and class members. Unauthorized individuals can now easily access the Personal Information of Plaintiff and class members.

D. HSG Failed to Comply with HIPAA Requirements

51. HSG is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

52. HSG is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

53. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

54. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

[5] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

55. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

56. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

57. HIPAA's Security Rule requires HSG to do the following:

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

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

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

d. Ensure compliance by its workforce.

58. HIPAA also requires HSG to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

59. Additionally, HSG is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

60. HIPAA and HITECH also obligated HSG to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

61. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires HSG to provide notice of the Data Breach to each affected individual "*without unreasonable delay and in no case later than 60 days following discovery of the breach*."[6]

62. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

63. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

64. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost-effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements

[6] *Breach Notification Rule*, U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last accessed on May 21, 2024) (emphasis added).

of the Security Rule." U.S. Department of Health & Human Services, Security Rule Guidance Material.[7] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." U.S. Department of Health & Human Services, Guidance on Risk Analysis.[8]

E. HSG Failed to Follow FTC Guidelines

65. HSG was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

66. The 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.

67. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

[7] *Security Rule Guidance Material*, U.S. Department of Health & Human Services, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed on May 21, 2024).

[8] *Guidance on Risk Analysis*, U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed on May 21, 2024).

understand their network's vulnerabilities; and implement policies to correct any security problems.

68. 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.

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

70. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect 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 FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

71. These FTC enforcement actions include actions against healthcare providers and partners like HSG. *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.").

72. HSG failed to properly implement basic data security practices.

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

74. HSG was at all times fully aware of its obligation to protect the Personal Information about whom it stored Personal Information. HSG was also aware of the significant repercussions that would result from its failure to do so.

F. HSG Failed to Comply with Industry Standards

75. As described above, experts studying cybersecurity routinely identify healthcare providers and their business associates as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

76. Several best practices have been identified that at a minimum should be implemented by HIPAA covered business entities like HSG, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

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

78. HSG 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.

79. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and HSG failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

G. HSG Owed Plaintiff and Class Members a Duty to Safeguard Their Personal Information

80. In addition to its obligations under federal and state laws, HSG owed a duty to Plaintiff and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. HSG owed a duty to Plaintiff and class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Personal Information of Plaintiff and class members.

81. HSG owed a duty to Plaintiff and class members to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees and others who accessed Personal Information within its computer systems on how to adequately protect Personal Information.

82. HSG owed a duty to Plaintiff and class members to implement processes that would detect a compromise of Personal Information in a timely manner.

83. HSG owed a duty to Plaintiff and class members to act upon data security warnings and alerts in a timely fashion.

84. HSG owed a duty to Plaintiff and class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

85. HSG owed a duty of care to Plaintiff and class members because they were foreseeable and probable victims of any inadequate data security practices.

86. HSG breached its obligations to Plaintiff and class members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. HSG's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect Personal Information;

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

d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

e. Failing to sufficiently train its employees and vendors regarding the proper handling of Personal Information;

f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

g. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and

h. Otherwise breaching its duties and obligations to protect Plaintiff's and class members' Personal Information.

87. HSG negligently and unlawfully failed to safeguard Plaintiff's and class members' Personal Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Personal Information.

88. Had HSG remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and class members' confidential Personal Information.

H. HSG Knew That Criminals Target PII/PHI from Healthcare Entities

89. HSG's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

90. At all relevant times, HSG knew, or should have known, Plaintiff's and all other class members' PII/PHI was a target for malicious actors. Despite such knowledge, HSG failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and class members' Personal Information from cyberattacks that HSG should have anticipated and guarded against.

91. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[9]

92. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found there were 956

[9] *9 reasons why healthcare is the biggest target for cyberattacks*, SwivelSecure, https://swivelsecure.com/solutions/ healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last accessed May 30, 2024).

medical data breaches in 2022 with over 59 million patient records exposed. This is an increase from the 905 medical data breaches that Protenus compiled in 2021.[10]

93. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[11]

94. Healthcare related breaches, in particular, have continued to rapidly increase because electronic patient data is seen as a valuable asset. In fact, entities that store patient information "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[12]

95. A 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[13]

96. Personal Information is a valuable property right.[14] The value of Personal

---

[10] *2022 Breach Barometer*, Protenus (2022), available at https://www.protenus.com/breach-barometer-report.

[11] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

[12] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on May 21, 2024).

[13] *Cost of a Data Breach Report 2022*, IBM Security (July 2022), available at https://www.ibm.com/downloads/cas/3R8N1DZJ.

[14] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP Advances in Information and Communication Technology (May 2015), available at https://www.researchgate.net/publication/283668023 ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and

Information as a commodity is measurable.[15] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[17] It is so valuable to identity thieves that once Personal Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

97. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, SSNs, Personal Information, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

98. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[18] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[19] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority

---

preferences as possible...").

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

[16] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, OECD Publishing (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

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

[18] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech Magazine (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[19] *Id.*

of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[20]

99. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[22] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[23] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[24] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen SSN or credit card number.[25]

100. Criminals can use stolen Personal Information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[26] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power

---

[20] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.
[21] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[22] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[23] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC Magazine (July 16, 2013), https://www.scmagazine.com/news/ breach/health- insurance-credentials-fetch-high-prices-in-the-online-black-market.
[24] *In the Dark*, VPNOverview.com, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 21, 2024).
[25] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI Cyber Division (Apr. 8, 2014), https://nsarchive.gwu.edu/document/18867-national-security-archive-department-justice.
[26] *See* note 18, *supra*.

of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[27]

101. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[28]

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

103. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[29]

104. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to

---

[27] *Id.*

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

[29] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

ransomware criminals … because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[30]

105. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[31]

106. HSG was on notice that the FBI has recently 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)."[32]

107. The American Medical Association ("AMA") has also warned healthcare companies about the importance 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.[33]

108. As implied by the above AMA quote, stolen Personal Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff

---

[30] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[31] *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.
[32] 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-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last accessed May 21, 2024).
[33] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, American Medical Association (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

and class members.

109. HSG was on notice that the federal government has been concerned about healthcare company data encryption practices. HSG knew its employees accessed and utilized protected health information in the regular course of their duties, yet it appears that information was not encrypted.

110. The Office for Civil Rights ("OCR") urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, OCR's deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[34]

111. Additionally, as companies became more dependent on computer systems to run their business,[35] e.g., working remotely as a result of the COVID-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[36]

112. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on HSG's server(s), amounting to potentially hundreds of thousands of

[34] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Department of Health and Human Services, (Apr. 22, 2014), https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

[35] *Implications of Cyber Risk for Financial Stability*, Board of Governors of the Federal Reserve System, (May 12, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.

[36] *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, Picus Security, (March 24, 2022), https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.

individuals' detailed Personal Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

113. As a HIPAA covered business associate, HSG knew or should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Personal Information stored in its unprotected files.

114. The injuries to Plaintiff and class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Personal Information of Plaintiff and class members.

115. The ramifications of HSG's failure to keep secure the Personal Information of Plaintiff and class members are long lasting and severe. Once Personal Information is stolen—particularly SSNs and PHI—fraudulent use of that information and damage to victims may continue for years.

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

116. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[37]

117. With access to an individual's Personal Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the

[37] *See What to Know About Identity Theft*, Federal Trade Commission Consumer Advice (April 2021) https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed on May 21, 2024).

victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[38] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and class members.

118. 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.

119. 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 SSN. 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 can be the starting point for these additional targeted attacks on the victim.

120. One such example of criminals piecing together bits and pieces of compromised Personal Information for profit is the development of "Fullz" packages.[39] With "Fullz" packages,

---

[38] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 30, 2024).

[39] "Fullz" is jargon for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, SSN, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's

cyber-criminals can cross-reference two sources of Personal Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

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

122. The existence and prevalence of "Fullz" packages means that the Personal Information stolen as a direct result of the Data Breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other class members.

123. Thus, even if certain information was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

124. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

125. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on dark web black markets for years.

---

knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/.

126. Cybercriminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data 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.[40]

127. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

128. The Personal Information exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[41]

129. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[42]

130. Theft of SSN also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of his or her SSN, and a new identification number will

---

[40] *Report to Congressional Requesters: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, United States Government Accountability Office (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.
[41] Ari Lazarus, *How fast will identity thieves use stolen info?*, Military Consumer (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.
[42] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, Identity Theft Resource Center (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

not be provided until after the victim has suffered the harm. In other words, preventative action to defend against the possibility of misuse of an SSN is not permitted.

131. Even then, a new SSN may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[43]

132. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[44]

133. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[45]

134. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information

[43] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.
[44] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[45] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Network World (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—including names and SSNs.

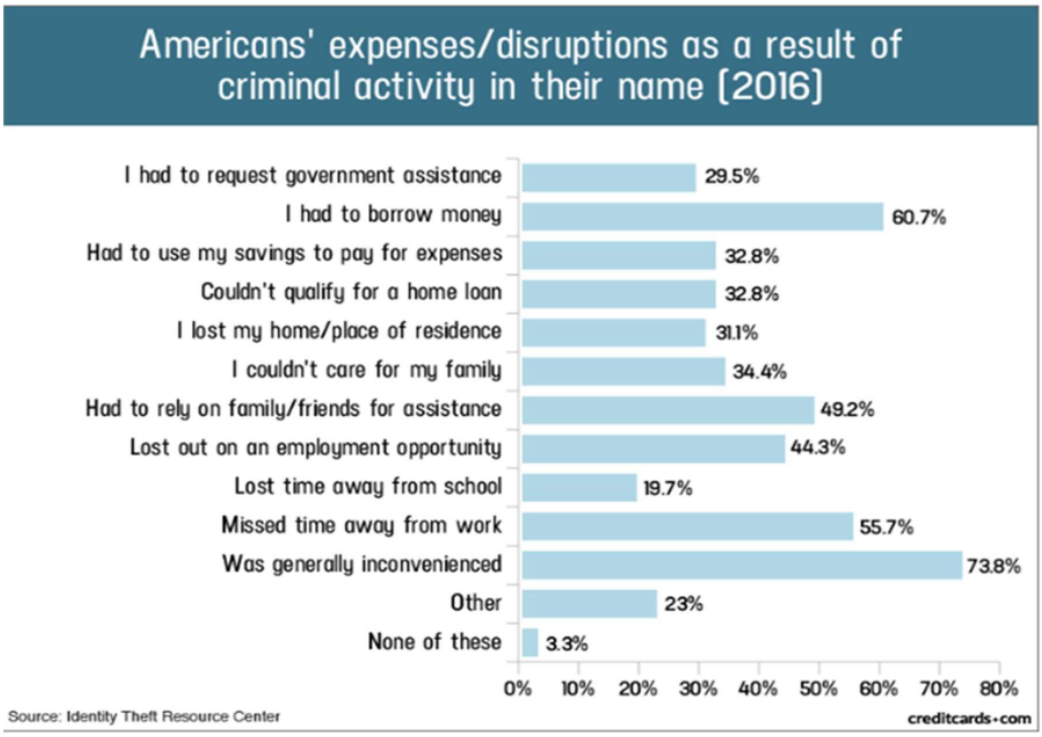
135. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her SSN 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.

136. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[46]

137. It is within this context that Plaintiff and all other class members must now live with the knowledge that their Personal Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

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

[46] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.



139. Victims of the Data Breach, like Plaintiff and class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[47]

140. As a direct and proximate result of the Data Breach, Plaintiff and class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and class members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely

[47] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission, (Sept. 2013), available at http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

141. Plaintiff and class members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including Personal Information;

b. Improper disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Personal Information being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential information used against them by spam callers to defraud them;

e. Damages flowing from HSG's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' Personal Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

142. Moreover, Plaintiff and class members have an interest in ensuring that their Personal Information, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiff's and class members' Personal Information.

143. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, HSG knew or should have known about these dangers and strengthened its data security accordingly. HSG was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

J. The Data Breach Was Foreseeable and Preventable

144. Data disclosures and data breaches are preventable.[48] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[49] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[50]

[48] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012).
[49] *Id.* at 17.
[50] *Id.* at 28.

145. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner *so that a data breach never occurs*."[51]

146. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[52]

147. Plaintiff and class members entrusted their Personal Information to HSG. Plaintiff and class members understood and expected that HSG or anyone in HSG's position would safeguard their Personal Information against cyberattacks, delete or destroy Personal Information that HSG was no longer required to maintain, and timely and accurately notify them if their Personal Information was compromised.

K. Plaintiff's and Class Members' Damages

148. To date, HSG has done nothing to provide Plaintiff and class members with relief for the damages they have suffered as a result of the Data Breach. HSG only offered minimal credit monitoring services, but it did not disclose how it determined eligibility. Not only did HSG fail to provide any ongoing credit monitoring or identity protection services for all individuals impacted by the Data Breach, but the credit monitoring does nothing to compensate class members for damages incurred and time spent dealing with the Data Breach.

149. Plaintiff and class members have been damaged by the compromise of their Personal Information in the Data Breach.

---

[51] *Id.* (emphasis added).

[52] *See How to Protect Your Networks from RANSOMWARE*, at 3, FBI.gov, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed May 30, 2024).

150. As a direct and proximate result of HSG's conduct, Plaintiff and class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

151. Plaintiff and class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Personal Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and class members.

152. Plaintiff and class members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

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

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and

fraudulent activity in their name;

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

f. Closely reviewing and monitoring SSNs, bank accounts, and credit reports for unauthorized activity for years to come.

154. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiff and class members' Personal Information.

155. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per class member. This is a reasonable and necessary cost to monitor to protect class members from the risk of identity theft that arose from HSG'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 HSG's failure to safeguard their Personal Information.

156. Plaintiff and class members suffered actual injury from having their Personal Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their Personal Information, a form of property that HSG obtained from Plaintiff and class members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

157. Further, as a result of Defendant's conduct, Plaintiff and class members are forced to live with the anxiety that their Personal Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

158. As a direct and proximate result of HSG's actions and inactions, Plaintiff and class members have suffered a loss of privacy and are at a present, imminent, and increased risk of future

harm.

159. Moreover, Plaintiff and class members have an interest in ensuring that their Personal Information, which is believed to remain in the possession of HSG, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Personal Information is not accessible online, is properly encrypted, and that access to such data is password protected.

160. Many failures laid the groundwork for the occurrence of the Data Breach, starting with HSG's failure to incur the costs necessary to implement adequate and reasonable cybersecurity training, procedures, and protocols that were necessary to protect Plaintiff's and class members' Personal Information.

161. HSG maintained the Personal Information in an objectively reckless manner, making the Personal Information vulnerable to unauthorized disclosure.

162. HSG knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would result if Plaintiff's and class members' Personal Information was stolen, including the significant costs that would be placed on Plaintiff and class members as a result of the breach.

163. The risk of improper disclosure of Plaintiff's and class members' Personal Information was a known risk to HSG, and thus HSG was on notice that failing to take necessary steps to secure Plaintiff's and class members' Personal Information from that risk left the Personal Information in a dangerous condition.

164. HSG disregarded the rights of Plaintiff and class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the Personal Information was protected against unauthorized intrusions; (ii) failing

to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and class members' Personal Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and class members prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

165. Plaintiff brings this class action individually and on behalf of all members of the following class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23:

Nationwide Class

All persons in the United States whose Personal Information was compromised in the Data Breach disclosed by Healthcare Services Group, Inc., including all who are sent notice of the Data Breach.

166. Alternatively, or in addition to the nationwide class, Plaintiff seek to represent the following state class:

Iowa Class

All persons in Iowa whose Personal Information was compromised in the Data Breach disclosed by Healthcare Services Group, Inc., including all who are sent notice of the Data Breach.

167. Excluded from the class(es) are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and any and all federal, state, or local governments; and the judge(s) presiding over this matter and the clerks and family members of said judge(s).

168. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

169. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Plaintiff's 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.

170. **Numerosity**: The members in the class are so numerous that joinder of all class members in a single proceeding would be impracticable. As noted above, according to Defendant's disclosures, over 600,000 individuals' Personal Information was exposed in the Data Breach. The class members are identifiable within Defendant's records inasmuch as Defendant has already provided them with notification of the breach.

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

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

b. Whether the computer systems and data security practices employed by HSG to protect Plaintiff's and class members' Personal Information violated the FTC Act and/or HIPAA, and/or state laws and/or HSG's other duties discussed herein;

c. When HSG actually learned of the Data Breach;

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

e. Whether Plaintiff and class members suffered injury as a proximate result of HSG's negligent actions or failures to act;

f. Whether HSG failed to exercise reasonable care to secure and safeguard Plaintiff's and class members' Personal Information;

g. Whether HSG adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and class members;

i. Whether HSG's actions and inactions alleged herein constitute gross negligence;

j. Whether HSG breached its duties to protect Plaintiff's and class members' Personal Information; and

k. Whether Plaintiff and all other members of the class are entitled to damages and the measure of such damages and relief.

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

173. **Typicality**: Plaintiff's claims are typical of the claims of the class. Plaintiff, like all proposed members of the class, had Personal Information compromised in the Data Breach. Plaintiff and class members were injured by the same wrongful acts, practices, and omissions

committed by HSG, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all class members.

174. **Adequacy**: Plaintiff will fairly and adequately protect the interests of the class members. Plaintiff is an adequate representative of the class and has no interests adverse to, or in conflict with, the class that Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

175. **Superiority**: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against HSG, so it would be impracticable for class members to individually seek redress from HSG's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

176. The nature of this action and the nature of laws available to Plaintiff and class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and class members for the wrongs alleged because HSG would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual class member with superior financial and legal resources; the

costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the class and will establish the right of each class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

177. The litigation of the claims brought herein is manageable. HSG's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

178. Adequate notice can be given to class members directly using information maintained in Defendant's records.

179. Unless a class-wide injunction is issued, HSG may continue in its failure to properly secure the Personal Information of class members, HSG may continue to refuse to provide proper notification to class members regarding the Data Breach, and HSG may continue to act unlawfully as set forth in this complaint.

180. Further, HSG has acted or refused to act on grounds generally applicable to the class and, accordingly, final injunctive or corresponding declaratory relief with regard to the class members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and all Classes)

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

182. HSG collected the Personal Information of Plaintiff and class members in the ordinary course of providing services directly or indirectly to Plaintiff and class members.

183. HSG owed a duty to Plaintiff and all other class members to exercise reasonable care in safeguarding and protecting their Personal Information in its possession, custody, or control. HSG's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach. HSG's duties arose under common law, HIPAA and FTC guidance.

184. HSG knew, or should have known, the risks of collecting and storing Plaintiff's and class members' Personal Information and the importance of maintaining secure systems. HSG knew, or should have known, of the many data breaches that targeted healthcare service providers in recent years.

185. Given the nature of HSG's business, the sensitivity and value of the Personal Information it maintains, and the resources at its disposal, HSG should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

186. HSG breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Personal Information entrusted to it—including Plaintiff's and class members' Personal Information.

187. It was reasonably foreseeable to HSG that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' Personal Information by failing to

design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and class members' Personal Information to unauthorized individuals.

188. HSG's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between HSG and patients. HSG was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and class members from a data breach.

189. HSG'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 HSG is bound by industry standards to protect confidential Personal Information.

190. But for HSG's negligent conduct or breach of the above-described duties owed to Plaintiff and class members, their Personal Information would not have been compromised.

191. As a result of HSG's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Personal Information; (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the value of their Personal Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or

attempted fraud.

192. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

193. Plaintiff and class members are also entitled to injunctive relief requiring HSG to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all class members.

COUNT II
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and all Classes)

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

195. Plaintiff and class members either directly or indirectly gave HSG their Personal Information in confidence, believing that HSG would protect that information. Plaintiff and class members would not have provided HSG with this information had they known it would not be adequately protected. HSG's acceptance and storage of Plaintiff's and class members' Personal Information created a fiduciary relationship between HSG and Plaintiff and class members. In light of this relationship, HSG must act primarily for the benefit of Plaintiff and class members, which includes safeguarding and protecting Plaintiff's and class members' Personal Information.

196. HSG accepted and used Plaintiff's and class members' Personal Information for its own pecuniary benefit and accepted the Personal Information with full knowledge of the need to maintain it as confidential, the need to implement appropriate data security measures, and the significant harm that would result to Plaintiff and class members if the confidentiality of their Personal Information was breached.

197. HSG was in a superior position of trust and authority to Plaintiff and class members.

198. Plaintiff and class members had no way to ensure that HSG's data security measures were adequate and no way to influence or verify the integrity of HSG's data security posture.

199. HSG has a fiduciary duty to act for the benefit of Plaintiff and class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and class members' Personal Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the Personal Information of Plaintiff and class members it collected. HSG also breached its fiduciary duty by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

200. As a direct and proximate result of HSG's breaches of its fiduciary duties, Plaintiff and class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Personal Information, which remains in HSG's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Personal Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud; (viii) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and class members; and (ix) the diminished value of HSG's services they received.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and all Classes)

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

202. This claim is pleaded in the alternative to any current or future contract claims, pursuant to Fed. R. Civ. P. 8(d).

203. Plaintiff and class members conferred a monetary benefit, directly or indirectly, upon HSG in the form of monies paid for services or other services.

204. HSG accepted or had knowledge of the benefits conferred upon it by Plaintiff and class members. HSG also benefitted from the receipt of Plaintiff's and class members' Personal Information.

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

206. Under principles of equity and good conscience, HSG should not be permitted to retain the money belonging to Plaintiff and class members because HSG failed to adequately implement the data privacy and security procedures for itself that Plaintiff and class members paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

207. HSG should be compelled to provide for the benefit of Plaintiff and class members all unlawful proceeds received by it as a result of its misconduct and the Data Breach.

COUNT IV
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiff and all Classes)

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

209. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

210. HSG owes a duty of care to Plaintiff and class members that require it to adequately secure Plaintiff's and class members' Personal Information.

211. HSG still possesses the Personal Information of Plaintiff and class members.

212. HSG has not satisfied its contractual obligations and legal duties to Plaintiff and class members.

213. Actual harm has arisen in the wake of the Data Breach regarding HSG's contractual obligations and duties of care to provide security measures to Plaintiff and class members. Further, Plaintiff and class members are at risk of additional or further harm due to the exposure of their Personal Information and HSG's failure to address the security failings that led to such exposure.

214. There is no reason to believe that HSG's employee training and security measures are any more adequate now than they were before the breach to meet HSG's contractual obligations and legal duties.

215. Plaintiff, therefore, seek a declaration (1) that HSG's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, HSG must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Prohibit HSG from engaging in the wrongful and unlawful acts described herein;

b. Ordering that HSG engage internal security personnel to conduct testing, including audits on HSG's systems, on a periodic basis, and ordering HSG to promptly correct any problems or issues detected by such third-party security auditors;

c. Requiring HSG 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;

d. Ordering that HSG engage third-party security auditors and internal personnel to run automated security monitoring;

e. Ordering that HSG audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

f. Ordering that HSG purge, delete, and destroy, in a reasonably secure manner, any Personal Information not necessary for its provision of services;

g. Ordering that HSG conduct regular database scanning and security checks; and

h. Prohibiting HSG from maintaining Personal Information of Plaintiff and class members on a cloud-based database;

i. Requiring HSG to segment data by, among other things, creating firewalls and access controls so that if one area of HSG's network is compromised, hackers cannot gain access to other portions of HSG's systems;

j. Ordering that HSG routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive Personal Information, including but not limited to, patient personally identifiable information and patient protected health information;

k. Requiring HSG to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding paragraphs, as well as randomly and periodically testing employees compliance with HSG's policies, programs, and systems for protecting personal identifying information;

l. Requiring HSG to meaningfully educate all class members about the threats 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;

m. Requiring HSG to implement logging and monitoring programs sufficient to track traffic to and from HSG'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 HSG'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;

n. Such other and further relief as this Court may deem just and proper.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the class, respectfully requests that the Court enter judgment in Plaintiff's favor and against HSG as follows:

A. Certifying the class(es) as requested herein, designating Plaintiff as class representative, and appointing Plaintiff's counsel as Class Counsel;

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

C. Awarding Plaintiff and the class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, individually and on behalf of the class, seeks appropriate injunctive relief designed to prevent HSG from experiencing another data breach by adopting and implementing best data security practices to safeguard Personal Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

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

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

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims so triable.

Dated: August 27, 2024

Respectfully submitted,

/s/ Andrew W. Ferich
Andrew W. Ferich (ID No. 313696)
Alyssa D. Brown (*pro hac vice* to be filed)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com
abrown@ahdootwolfson.com

Benjamin F. Johns (ID No. 201373)
Samantha E. Holbrook (ID No. 311829)
SHUB JOHNS & HOLBROOK LLP
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Telephone: (610) 477-8380
Facsimile: (856) 210-9088
bjohns@shublawyers.com
sholbrook@shublawyers.com

Counsel for Plaintiff and the Putative Class