Exhibit A

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

REBECCA RICHARDS, HAROLD HENDERSON, STACY PETRILLO, and **STANLEY WILLIAMSON**, individually and on behalf of all others similarly situated, Plaintiffs, v. **HEALTHCARE SERVICES GROUP, INC.** Defendant.	**Case No. 2:25-cv-04908-JDW** **CONSOLIDATED COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Rebecca Richards, Harold Henderson, Stacy Petrillo, and Stanley Williamson ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through the undersigned attorneys, bring this consolidated class action against Defendant Healthcare Services Group, Inc. ("HSG" or "Defendant") and complain and allege upon personal knowledge as to their own actions and their counsels' investigations, and upon information and good faith belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action against HSG for its failure to secure and safeguard the personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Private Information") of approximately 624,496 individuals ("Class Members").

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

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

4. On or about August 25, 2025, HSG publicly reported that its computer systems were subjected to unauthorized access *nearly one year earlier*, between September 27, 2024 and October 3, 2024 (the "Data Breach").[1] HSG did not immediately detect and stop the intrusion, but learned of it days later, on October 7, 2024.[2] HSG's initial notice indicated that the Data Breach exposed the PII and PHI of 624,496 individuals.[3]

5. Despite having knowledge of the Data Breach as early as October 7, 2024, HSG did not alert any of the individuals affected until it mailed notice to them on August 25, 2025—well over ten months after it discovered the Breach.

6. According to HSG and public reports, the exposed Private Information included names, Social Security numbers, driver's license numbers, state identification numbers, financial account details, full access credentials, and medical and health insurance information.[4][5]

7. HSG's reporting acknowledges that Plaintiffs' and Class Members' Private Information was unlawfully accessed by the cybercriminals, but HSG did not disclose how HSG discovered the files on its computer systems were impacted, the means and mechanism of the

[1] Data Breach Notifications, Office of the Maine Att'y Gen., https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/9a82ac2b-5379-462d-acd6-26a3b3bd0b30.html (last visited Dec. 19, 2025); *see also* Letter template from Healthcare Services Group, https://www.maine.gov/cgi-bin/agviewerad/ret?loc=2964 (last visited Dec. 19, 2025) [hereinafter "Data Breach Notice"].

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] Data Security Breach Reports, Office of the Attorney General of Texas, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage

cyberattack, the reason for the nearly eleven-month delay in disclosing the Data Breach, how it determined that the PII and 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 Private Information from the foreseeable threat of a cyberattack.

9. The Data Breach was perpetrated by a known cybercriminal group called Team Underground a/k/a Underground, which advertised the data taken from HSG's network on its dark web leak site in October 2024 and claimed to have stolen and published 1.1 terabytes of confidential company and personal records.

10. Plaintiffs bring this class action lawsuit individually and on behalf of those similarly situated to address HSG's inadequate safeguarding of Plaintiffs' and Class Members' Private Information that it collected and maintained and for failing to provide prompt and adequate notice to Plaintiffs and Class Members.

11. Plaintiffs bring claims for negligence, breach of implied contract, breach of contracts to which Plaintiffs and Class Members were intended third-party beneficiaries, breach of fiduciary duty, unjust enrichment, violations of the New Jersey Consumer Fraud Act, violations of the Washington Consumer Protection Act, and declaratory and injunctive relief. To remedy these violations of law, Plaintiffs and Class Members seek actual damages, statutory damages, restitution, 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

Plaintiffs

12. Plaintiff Rebecca Richards is a citizen and resident of Auburn, Washington.

13. Plaintiff Harold Henderson is a citizen and resident of Houston, Texas.

14. Plaintiff Stacy Petrillo is a citizen and resident of Williamstown, New Jersey.

15. Plaintiff Stanley Williamson is a citizen and resident of Gainesville, Florida.

Defendant

16. 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

17. 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, including Plaintiffs Richards, Henderson, Petrillo, and Williamson, there are more than 100 members of the class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs.

18. This Court has personal jurisdiction over HSG because HSG maintains its principal place of business in Pennsylvania, conducts substantial business in Pennsylvania and within 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.

19. 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 Plaintiffs' and Class Members' Private Information in this District, and this District is where a substantial part of the acts, omissions, and events giving rise to Plaintiffs' claims occurred.

FACTUAL ALLEGATIONS

A. Overview of HSG Health

20. Founded in 1976, HSG is a Bensalem-based entity offering 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.

21. HSG 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.

22. In the regular course of its business, HSG collects and maintains Private Information. As a regular part of its business, HSG requires individuals to provide personal information, directly or indirectly, before providing its services. HSG also collects Private Information from its employees as a condition of their employment. HSG stores this information unencrypted and in an internet accessible environment.

23. HSG is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security

Rule[6] and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

24. In its Privacy Policy, HSG affirms that it "respects the privacy of our users" and would protect the Private Information from unauthorized disclosures;[7] yet, HSG maintained inadequate security measures which allowed the Data Breach to occur. It then waited nearly eleven months after discovering the Data Breach to disclose that Private Information had been compromised.

25. Plaintiffs and Class Members are current and former employees, patients or patients of HSG's customers, and/or received health-related or other services from HSG, or are otherwise affiliated or transacted with HSG, and entrusted HSG with their Private Information.

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

---

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

[7] Healthcare Services Group, Inc., *Privacy Policy*, WWW.HCSGCORP.COM, https://www.hcsgcorp.com/privacy-policy/ (last updated Apr. 23, 2025).

27. Defendant could have prevented or mitigated the consequences of the Data Breach by limiting access to sensitive information to only necessary employees, requiring multi-factor authentication to verify access credentials, encrypting data at rest and in transit, monitoring its systems for signs of unusual activity or the transfer of large volumes of data, and regularly rotating passwords. As evidenced by the Data Breach, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

B. HSG Is a HIPAA-Covered Business Entity

28. HSG is a HIPAA-covered business associate that provides services to healthcare providers and, through those providers, to Plaintiffs and Class Members. As a condition of benefiting from HSG's services, HSG requires that Plaintiffs and Class Members (or their medical providers) provide it with highly sensitive Private Information. Due to the nature of HSG's business of providing healthcare-related services, HSG would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

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

30. Plaintiffs and Class Members are and were individuals whose sensitive information was maintained by HSG, and who directly or indirectly entrusted HSG with their Private

Information. Plaintiffs and Class Members reasonably expected that HSG would safeguard and keep their Private Information confidential.

C. The Data Breach Compromised Plaintiffs' and Class Members' Private Information

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

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

33. 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 full access credentials.

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

35. 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 Private Information had been accessed, and, of particular importance to Plaintiffs and Class Members, what steps HSG took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks.

36. Notwithstanding HSG's public acknowledgment that Private Information "may have" been accessed and copied by an unauthorized party, it is evident that unauthorized criminal actors did, in fact, access HSG's network and thus Plaintiffs' and Class Members' Private Information in an attack designed to acquire that sensitive, confidential, and valuable information.

37. In the context of notice of data breach letters of this type, Defendant's use of the phrase "may have been subject to unauthorized access" is misleading lawyer language. Companies only send notice letters because data breach notification laws require them to do so. And such letters are only sent to those persons who Defendant itself has a reasonable belief that their private information was accessed or acquired by an unauthorized individual or entity. Defendant cannot hide behind legalese—by sending a notice of data breach letter to Plaintiff and Class Members, it admits that Defendant itself has a reasonable belief that Plaintiffs' and Class Members' names, dates of birth, and Social Security numbers were accessed or acquired by an unknown actor—aka cybercriminals.

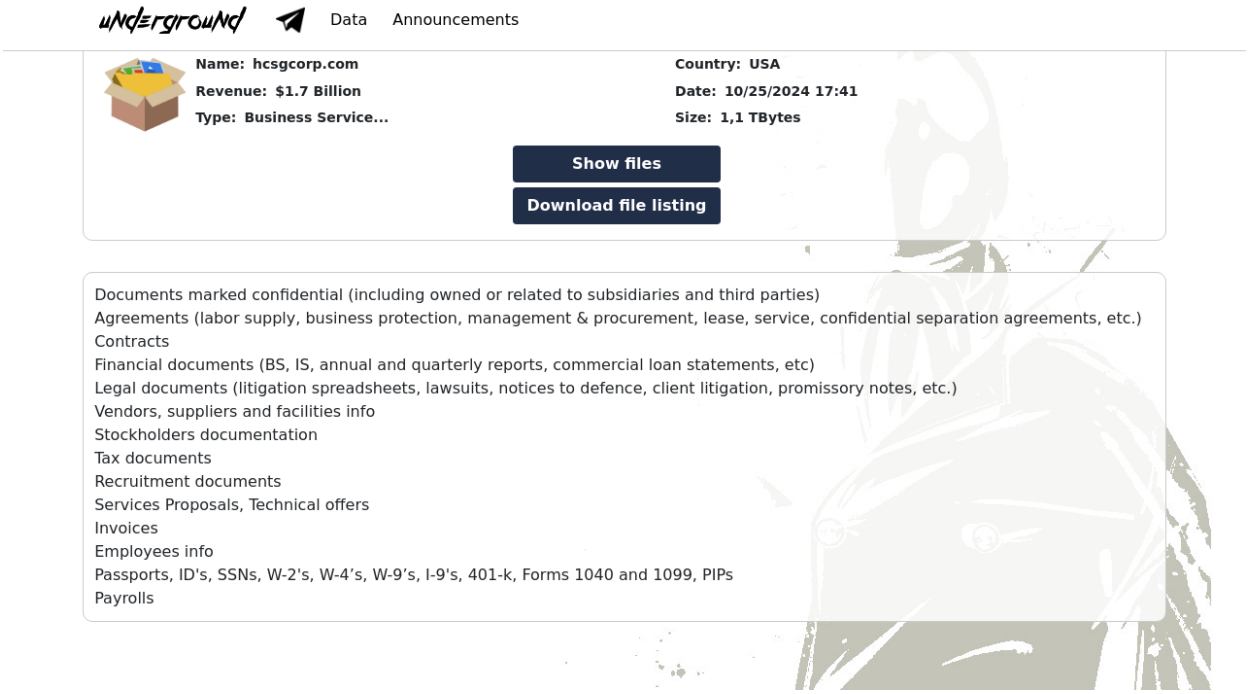
38. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook any efforts to contact the approximately 624,496 Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

39. Indeed, the Identity Theft Research Center's 2024 Annual Data Breach Report notes that, "approximately 70 percent of cyberattack-related breach notices did not include attack information, compared to 58 percent in 2023. In 2019 and previous years, ~100 percent of breach notices included attack vector information." Eva Velasquez, CEO of the Identity Theft Resource Center, remarked that "[w]ith a near-record number of compromises and over 1.3 billion victim notices, often tied to inadequate cyber practices, we are also seeing an increase in notices that provide limited actionable information for victims."[8]

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

40. In a 2019 study, researchers found that "97 percent of the 161 sampled notifications were difficult or fairly difficult to read based on readability metrics, and that the language used in them may have contributed to confusion about whether the recipient of the communication was at risk and should take action." The researchers went on to note that breached entities "use hedge terms that downplay risk—using phrases like 'you might be affected' and 'you are likely to be affected'" as "[f]or most companies, those notifications are only seen as a requirement for complying with data breach notification laws rather than a way to educate and protect their customers."[9]

41. In October 2024, a cybercriminal group known as Team Underground a/k/a Underground posted on its dark web leak site that it stole 1.1 terabytes of confidential company and personal records from HSG's computer systems, as demonstrated in the image below:



[9] Yixin Zou, *Companies Send Confusing Alerts About Data Breaches*, FUTURITY (May 19, 2019), available at https://www.futurity.org/data-breaches-notifications-2066072/

42. Underground's leak site advertised for sale the following types of information taken from HSG's network:

- Personal Identifiers: Names, Social Security numbers, passports, government-issued IDs;
- Employee Data: W-2s, W-4s, W-9s, I-9s, payroll records, performance improvement plans (PIPs);
- Medical/Insurance Data: Health and insurance records tied to employees and patients;
- Financial Records: Bank statements, tax forms (1040, 1099), 401(k) information; and
- Corporate Documentation: Contracts, agreements, stockholder records, litigation documents, tax records, proposals, technical offers, invoices, vendor/supplier details.

43. Underground is a known cybercriminal group that specializes in ransomware and data exfiltration, followed by public leaks on dedicated leak portals.

44. A ransomware attack is a type of cyberattack that is frequently used to target healthcare providers due to the sensitive patient data they maintain.[10] Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[11] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

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

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

45. Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[12] And even when companies pay for the return of data, attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[13]

46. The United States government and other law enforcement agencies almost always advise against paying a ransom demand, and that is because cybercriminals cannot be trusted to do what they promise they will do in exchange for a ransom.

47. There is no guarantee that the cybercriminals would honor their promises after being paid a ransom: the hackers could easily have re-copied the stolen data.[14]

48. Indeed, data breach targets that pay ransom demands often cannot substantiate any claimed destruction or return of the data in question.[15]

---

[12] *Id*.

[13] *Id*.

[14] Gary Guthrie, *Paying to delete stolen data doesn't always work out for the victim, new study suggests*, CONSUMERAFFAIRS (Nov. 5, 2020), https://www.consumeraffairs.com/news/paying-to-delete-stolen-data-doesnt-always-work-out-for-the-victim-new-study-suggests-110520.html [https://perma.cc/DMV2-JRFP].

[15] *See* Leo Kelion & Joe Tidy, *National Trust joins victims of Blackbaud hack*, BBC NEWS (July 30, 2020), https://www.bbc.com/news/technology-53567699 ("Although Blackbaud has said the cyber-criminals had provided confirmation that the stolen data was destroyed, one expert questioned whether such an assurance could be trusted. 'The hackers would know these people have a propensity to support good causes,' commented Pat Walshe from the consultancy Privacy Matters. 'This would be valuable information to fraudsters,' he added, 'who could use it to fool victims into thinking they were making further donations when in fact they would be giving away their payment card details.'") [https://perma.cc/NC7W-T9LJ]; *Phishing Scams Following Blackbaud Security Breach*, Mich. Dep't Att'y Gen., https://www.michigan.gov/ag/0,4534,7-359-81903_20942-540014--,00.html [https://perma.cc/E6K9-HVZZ].

49. The FBI recognizes the likelihood that cybercriminals will renege on their promises once a ransom is paid, explaining that it "does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data."[16]

50. Several media outlets and industry groups have likewise questioned reliance on promises made by cybercriminals.[17]

51. The damage has already been done. Plaintiffs' and Class Members' Private Information was taken by cybercriminals and listed for sale on the dark web to be used to commit wide-ranging fraud and identity theft, including tax fraud, opening of fraudulent accounts, impersonation, extortion, medical fraud, and much more.

52. The dark web is a part of the World Wide Web that is not accessible through traditional internet browsers. The term "dark web" is used to distinguish from the "clear web," the part of the World Wide Web that is readily accessible through traditional internet browsers. The dark web is accessed through The Onion Router ("Tor"), a privacy-focused communication system designed to enable anonymous internet browsing. It achieves this by routing web traffic through multiple volunteer-operated servers (relays), encrypting data at each step to ensure that both the user's location and browsing activity are difficult to trace. Tor uses a technique called "onion routing," where data is encrypted in layers like an onion. Each relay in the network peels away a

[16] *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI (Oct. 2, 2019), https://www.ic3.gov/Media/Y2019/PSA191002 [https://perma.cc/VX8P-TW7F].

[17] *See, e.g.*, Phil Muncaster, *US Data Breach Volumes Plummet 30% in 2020*, INFOSECURITY MAG. (Oct. 15, 2020), https://www.infosecurity-magazine.com/news/us-data-breach-volumes-plummet-30/ [https://perma.cc/2LYC-XDP6]; Zack Whittaker, *Decrypted: The Major Ransomware Attack You Probably Didn't Hear About*, TECHCRUNCH (Oct. 7, 2020), https://techcrunch.com/2020/10/07/decrypted-blackbaud-ransomware-attack-gets-worse/ [https://perma.cc/R8M4-FMMC].

layer of encryption before passing the data to the next relay. This ensures that no single relay knows both the origin and destination of the data.

53. The dark web poses significant challenges to cybersecurity professionals and law enforcement agencies. The dark web is legal to access and operate, and it has some legitimate applications and sites. But its hidden nature and employment of multi-level encryption make detecting and monitoring illegal activity difficult. Unlike the clear web, dark web sites do not advertise their existence. The anonymity of the dark web has led to the creation of a number of markets and forums which traffic in illegal merchandise and content, including stolen Private Information.[18]

54. Once stolen Private Information is posted on the dark web, it will most likely be distributed to multiple different groups and individuals, each of which can use that information for fraud and identity theft.[19]

55. This data lifecycle has also been confirmed with experiments. In 2015, researchers at BitGlass created a list of 1,568 phony names, Social Security numbers, credit card numbers, addresses, and phone numbers, rolled them in an Excel spreadsheet, and then "watermarked" it with their code that silently tracks access to the file.[20] The data was quickly spread across five

[18] *Crime and the Deep Web*, STEVENSON UNIV. ONLINE, https://www.stevenson.edu/online/about-us/news/crime-deep-web/ (last visited Dec. 19, 2025); *Defending Against Malicious Cyber Activity Originating from Tor*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (CISA), https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a (last updated Aug. 2, 2021).

[19] *The Dark Web and Cybercrime*, U.S. DEP'T OF HEALTH AND HUM. SERVS. (July 23, 2020), https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf.

[20] Kelly Jackson Higgins, *What Happens When Personal Information Hits the Dark Web*, DARK READING (Apr. 7, 2015), https://www.darkreading.com/cyberattacks-data-breaches/what-happens-when-personal-information-hits-the-dark-web; Kristin Finklea, *Dark Web*, NAT'L SEC. ARCHIVE (July 7, 2015), https://nsarchive.gwu.edu/media/21394/ocr; *Dark Web*, Cong. RSCH. SERV., https://crsreports.congress.gov/product/pdf/R/R44101 (last updated Mar. 10, 2017).

continents: North America, Asia, Europe, Africa, and South America. In the end, it was downloaded by 47 different parties. It was mainly downloaded by users in Nigeria, Russia, and Brazil, with the most activity coming from Nigeria and Russia.[21] This experiment demonstrated that data released on the dark web will quickly spread around the world.

56. Upon information and belief, the Private Information contained in the files accessed by cybercriminals was not encrypted, because, if properly encrypted, the attackers would have acquired unintelligible data and would not have "accessed and copied" Private Information.

57. The Data Breach reportedly impacted the protected health and other confidential information of 624,496 individuals.[22]

58. As a 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.

59. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of Plaintiffs and Class Members.

60. Due to HSG's inadequate security measures, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

[21] Pierluigi Paganini, *How Far Do Stolen Data Get in the Deep Web After a Breach?*, SECURITY AFFAIRS (Apr. 12, 2015), https://securityaffairs.com/35902/cyber-crime/propagation-data-deep-web.html.

[22] Data Breach Notice, *supra* note 1.

61. HSG had obligations created by HIPAA, statutory law, contract law, industry standards, and common law to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

62. Plaintiffs and Class Members entrusted their Private 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 Private 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.

63. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, HSG assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

64. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiffs and Class Members would not have allowed HSG or anyone in HSG's position to receive their Private Information had they known that HSG would fail to implement industry standard protections for that sensitive information.

65. As a result of HSG's negligent and reckless conduct, Plaintiffs' and Class Members' highly confidential and sensitive Private Information was left exposed to cybercriminals. The unencrypted Private Information of Plaintiffs and Class Members has already been posted for sale to identity thieves on the dark web and will further be misused for targeted marketing without the consent of Plaintiffs and Class Members. Unauthorized individuals and criminals can now easily misuse the Private Information of Plaintiffs and Class Members.

D. HSG Failed to Comply with HIPAA Requirements

66. 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.

67. HSG is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[23] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

69. 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.

70. 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.

71. "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.

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

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

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.

73. 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).

74. 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).

75. 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.

76. 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*."[24]

[24] *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Dec. 19,

77. 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).

78. 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).

79. 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. §§ 164.302-318. 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 of the Security Rule." U.S. Department of Health & Human Services, Security Rule Guidance Material.[25] 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.[26]

2025) (emphasis added).

[25] *Security Rule Guidance Material*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Dec. 19, 2025).

[26] *Guidance on Risk Analysis*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Dec. 19, 2025).

E. HSG Failed to Follow FTC Guidelines

80. 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).

81. 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.

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

83. 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.

84. 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.

85. 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.

86. 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.").

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

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

89. HSG was at all times fully aware of its obligation to protect the Private Information it collected from employees, clients, and patients. 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

90. 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.

91. 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.

92. 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.

93. HSG failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

94. 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 Plaintiffs and Class Members a Duty to Safeguard Their Private Information

95. In addition to its obligations under federal and state laws, HSG owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being

compromised, lost, stolen, accessed, and misused by unauthorized persons. HSG owed a duty to Plaintiffs 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 Private Information of Plaintiffs and Class Members.

96. HSG owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

97. HSG owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

98. HSG owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

99. HSG owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

100. HSG owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

101. HSG breached its obligations to Plaintiffs 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 vendors' 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 Private 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 vendors' data security practices;

e. Failing to sufficiently train its employees and vendors regarding the proper handling of Private 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 Plaintiffs' and Class Members' Private Information.

102. HSG negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

103. 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 Plaintiffs' and Class Members' confidential Private Information.

H. HSG Knew That Criminals Target Private Information from Healthcare Entities

104. 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.

105. At all relevant times, HSG knew, or should have known, Plaintiffs' and all other Class Members' Private Information 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 Plaintiffs' and Class Members' Private Information from cyberattacks that HSG should have anticipated and guarded against.

106. "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."[27]

107. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2025 report, the healthcare compliance company Bluesight found there were 1,160 medical data breaches in 2024, with over 300 million patient records exposed.[28]

108. 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 five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[29]

---

[27] *9 Reasons Why Healthcare Is the Biggest Target for Cyberattacks*, SWIVELSECURE, https://swivelsecure.com/solutions/ healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Dec. 19, 2025).

[28] *2025 Breach Barometer*, BLUESIGHT (2025), https://bluesight.com/wp-content/uploads/2025/02/2025-Breach-Barometer-Annual-Report.pdf;

[29] Jill Hughes, *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.

109. 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."[30]

110. A 2022 report released by IBM Security states that for twelve 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.[31]

111. Private Information is a valuable property right.[32] The value of Private Information as a commodity is measurable.[33] "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."[34] American companies are estimated to have spent over $19

[30] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGIT. HEALTH (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

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

[32] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFO. AND COMMC'N TECH. 26, 29 (2015), 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 preferences as possible...").

[33] *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.

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

billion on acquiring personal data of consumers in 2018.[35] It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

112. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, Private 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.

113. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[36] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[37] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority 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.[38]

114. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider,

---

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

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

[37] *Id.*

[38] 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.

or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[39]

115. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[40] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[41]

116. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data [to] open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers,

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

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

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

> having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[42]

117. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can sell for up to $1,000 online."[43]

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

> *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[44] (Emphasis added).

119. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being

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

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

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

issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[45]

120. The Social Security Administration further stresses that:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[46]

121. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[47]

122. A driver's license can be a critical part of a fraudulent, synthetic identity—which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[48]

123. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep

---

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

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

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

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

> a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

124. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[49] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[50]

125. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in by the New York Times.[51]

126. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[52] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[53] All-inclusive health insurance dossiers

---

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

[50] *Id.*

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

[52] Anita George, *Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs,* DIGIT. TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[53] 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/.

containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[54] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[55] According to a report released by the Federal Bureau of Investigation's (FBI) Cyber Division, criminals can sell healthcare records for fifty times the price of a stolen Social Security or credit card number.[56]

127. Criminals can use stolen Private Information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[57] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[58]

128. 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

[54] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/ breach/health- insurance-credentials-fetch-high-prices-in-the-online-black-market.

[55] *In the Dark*, VPNOVERVIEW.COM, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited May 21, 2024).

[56] *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.

[57] *See* Lowes, *supra* note 18.

[58] *Id.*

willing to pay a premium to purchase from privacy protective websites."[59]

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

130. 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, cybercriminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cybercriminals will no doubt lead to an escalation in cybercrime."[60]

131. 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 ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[61]

132. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[62]

133. HSG was on notice that the FBI has recently been concerned about data security in

---

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

[60] 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.

[61] 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.

[62] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack,* SEC. MAG. (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

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)."[63]

134. 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.[64]

135. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

136. 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.

137. 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

---

[63] Jim Finkle, *FBI Warns Healthcare Firms That They Are Targeted by Hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[64] Andis Robeznieks, *Cybersecurity: Ransomware Attacks Shut Down Clinics, Hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

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."[65]

138. Additionally, as companies became more dependent on computer systems to run their business,[66] 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.[67]

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

140. 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 Private Information stored in its unprotected files.

141. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

---

[65] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. DEP'T OF HEALTH & HUM. SERVS. (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.

[66] *Implications of Cyber Risk for Financial Stability*, BD. OF GOVERNORS OF THE FED. RSRV. SYS., (May 12, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.

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

142. The ramifications of HSG's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

I. Theft of Private Information Has Grave and Lasting Consequences for Victims

143. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[68]

144. With access to an individual's Private 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 Social Security number 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 victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[69] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

145. 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

[68] *See What to Know About Identity Theft*, F.T.C. CONSUMER ADVICE (April 2021), https://www.consumer.ftc.gov/articles/what-know-about-identity-theft.

[69] *See Warning Signs of Identity Theft*, F.T.C., https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 30, 2024).

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.

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

147. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[70] With "Fullz" packages, cybercriminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

148. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class

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

Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was 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.

149. The existence and prevalence of "Fullz" packages means that the Private Information stolen as a direct result of the Data Breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other Class Members.

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

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

152. Private 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.

153. 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.[71]

[71] *Report to Congressional Requesters: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

154. 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.

155. The Private 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.[72]

156. 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.[73]

157. Theft of Social Security numbers 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 Social Security number, and a new identification number will not be provided until after the victim has suffered the harm. In other words, preventative action to defend against the possibility of misuse of a Social Security number is not permitted.

[72] Ari Lazarus, *How Fast Will Identity Thieves Use Stolen Info?*, MIL. CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.

[73] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

158. Even then, a new Social Security number 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."[74]

159. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers 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 Jim 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."[75]

160. 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."[76]

161. 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

[74] 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.

[75] 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/.

[76] 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 Social Security numbers.

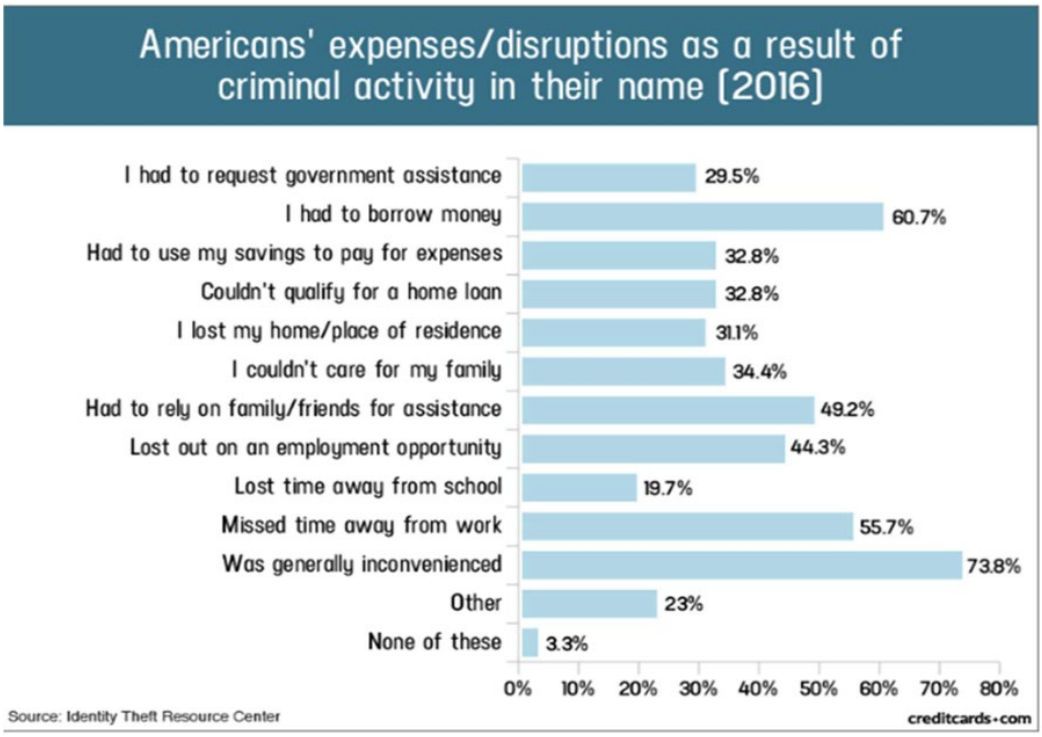
162. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual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

163. 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.[77]

164. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their Private 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.

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

[77] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9, 12 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.



166. Victims of the Data Breach, like Plaintiffs 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.[78]

167. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs 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

[78] *Guide for Assisting Identity Theft Victims*, F.T.C., (Sept. 2013), 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.

168. Plaintiffs 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 Private Information;

b. Improper disclosure of their Private Information;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Private 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' Private 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 Private Information; and

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

169. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private 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 Plaintiffs' and Class Members' Private Information.

170. 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

171. Data disclosures and data breaches are preventable.[79] 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."[80] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that

[79] *See generally* Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches are Preventable,* DATA BREACH AND ENCRYPTION HANDBOOK (2012) (explaining how to prevent data breaches).

[80] *Id.* at 17.

it is not compromised . . . ."[81]

172. "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*."[82]

173. 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."[83]

174. Plaintiffs and Class Members entrusted their Private Information to HSG. Plaintiffs and Class Members understood and expected that HSG or anyone in HSG's position would safeguard their Private Information against cyberattacks, delete or destroy Private Information that HSG was no longer required to maintain, and timely and accurately notify them if their Private Information was compromised.

K. Plaintiffs' and Class Members' Damages

175. To date, HSG has done nothing to provide Plaintiffs 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 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.

---

[81] *Id.* at 28.

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

[83] *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 visited May 30, 2024).

176. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

177. As a direct and proximate result of HSG's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs 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.

178. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

179. Plaintiffs 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.

180. Plaintiffs 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 Social Security numbers, bank accounts, and credit reports for unauthorized activity for years to come.

181. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

182. 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 Plaintiffs and Class Members would not need to bear but for HSG's failure to safeguard their Private Information.

183. Plaintiffs and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their Private Information, a form of property that HSG obtained from Plaintiffs 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.

184. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private 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.

185. As a direct and proximate result of HSG's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at a present, imminent, and increased risk of future harm.

186. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private 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 Private Information is not accessible online, is properly encrypted, and that access to such data is password protected.

187. 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 Plaintiffs' and Class Members' Private Information.

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

189. HSG knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would result if Plaintiffs' and Class Members' Private Information was stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of the breach.

190. The risk of improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to HSG, and thus HSG was on notice that failing to take necessary steps to secure Plaintiffs' and Class Members' Private Information from that risk left the Private Information in a dangerous condition.

191. HSG disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the Private 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 Plaintiffs' and Class Members' Private 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 Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

Plaintiffs' Injuries

Plaintiff Rebecca Richards

192. Plaintiff Rebecca Richards is a former employee of Defendant, having worked for HSG from April 2019 until December 2023.

193. As a condition of employment, Defendant required Plaintiff Richards to provide it with her Private Information. Defendant thus obtained and maintained Plaintiff Richards's Private Information.

194. Plaintiff Richards provided her Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to HSG's internal policies as well as state and federal law.

195. As a result, Plaintiff Richards was injured by Defendant's Data Breach.

196. Upon information and belief, Plaintiff Richards's information has not been compromised in any previous data breaches of which she is aware.

197. Upon information and belief, Defendant maintained Plaintiff Richards's Private Information after the employment relationship had ended.

198. Plaintiff Richards called the data breach hotline to confirm that her data was exposed in the data breach and, ultimately, she received a Data Breach Notice from Defendant, dated August 25, 2025, which confirmed that her information was impacted by the Data Breach.

199. Through its Data Breach, Defendant compromised Plaintiff Richards's Private Information, including her Social Security number, driver's license information, health insurance information, medical information, bank account and other financial information, and full access credentials.

200. On information and belief, Plaintiff Richards's Private Information was obtained by cybercriminals and has been, or will be, published on the dark web.

201. Once an individual's Private Information is for sale and accessible on the dark web, as Plaintiff Richards's Private Information is, or likely will be, as a result of the Breach, cybercriminals are able to use the stolen and compromised information to gather and steal even more information.

202. Plaintiff Richards has spent—and will continue to spend—significant time and effort monitoring her accounts, researching the Data Breach, contacting counsel, and calling the breach hotline to protect herself from identity theft. Defendant directed Plaintiff Richards to take those steps in its breach notice.

203. Since the Data Breach, Plaintiff Richards has spent approximately seventy-two hours researching the Data Breach, monitoring for suspicious activity, and changing her passwords.

204. Plaintiff Richards continues to spend approximately an hour a week attempting to mitigate the consequences of the Data Breach.

205. Plaintiff Richards fears for her personal financial security and worries about what information was exposed in the Data Breach.

206. Because of Defendant's Data Breach, Plaintiff Richards has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Richards's injuries are precisely the type of injuries that the law contemplates and addresses.

207. Plaintiff Richards suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

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

209. Plaintiff Richards suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Richards's Private Information right in the hands of criminals.

210. Because of the Data Breach, Plaintiff Richards anticipates spending considerable amounts of time and money to try and mitigate her injuries.

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

Plaintiff Harold Henderson

212. Plaintiff Harold Henderson is a former employee of Defendant.

213. As a condition of obtaining employment from Defendant, Plaintiff Henderson was required to provide Defendant with his Private Information.

214. As a result, Plaintiff Henderson was injured by Defendant's Data Breach.

215. Plaintiff Henderson received a Data Breach notice, dated August 25, 2025, indicating that his Private Information was exposed in the Breach.

216. Defendant was in possession of Plaintiff Henderson's Private Information before, during, and after the Data Breach.

217. Plaintiff Henderson reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Henderson would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

218. Plaintiff Henderson greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Henderson is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

219. Plaintiff Henderson stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts.

220. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

221. Nonetheless, as a result of the Data Breach, Plaintiff Henderson's Private Information is now in the hands of cybercriminals. Through its Data Breach, Defendant compromised Plaintiff Henderson's Private Information including his Social Security number,

driver's license information, health insurance information, medical information, bank account and other financial information, and full access credentials.

222. Plaintiff Henderson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Henderson will continue to be at present and ongoing increased risk of identity theft and fraud for years to come.

223. Plaintiff Henderson has spent between 40 and 50 hours researching the Data Breach, monitoring his accounts for suspicious activity, changing passwords, and requesting that his payment cards be replaced. Plaintiff Henderson continues to spend 10 to 20 hours a week attempting to mitigate the consequences of the Data Breach.

224. Following the Data Breach, around April of 2025, Plaintiff Henderson discovered fraudulent charges on his Chase Bank debit card. The charges were made at a Walmart for around $8 and then around $1,000, and Plaintiff Henderson did not make these charges. After this fraud occurred, Chase Bank issued Plaintiff Henderson a new debit card. Plaintiff Henderson also learned around May or June of 2025 that someone attempted to access his credit and that his credit score had decreased as a result.

225. On information and belief, Plaintiff Henderson's Private Information was obtained by cybercriminals and has been, or will be, published on the dark web. The fraudulent activity that Plaintiff has suffered further indicates such exposure.

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

227. As a direct and traceable result of the Data Breach, Plaintiff Henderson suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his Private Information; (d) emotional distress because identity thieves now possess his sensitive Private Information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and likely published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Henderson; and (g) other economic and non-economic harm.

Plaintiff Stacy Petrillo

228. Plaintiff Stacy Petrillo is a former HSG customer and HSG had access to her Private Information as a result of that relationship.

229. Plaintiff Petrillo received a notice letter from Defendant, dated August 25, 2025, informing her that her Private Information—including her Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

230. Plaintiff Petrillo is very careful with her Private Information.

231. Plaintiff Petrillo would not have provided her Private Information to Defendant had she known that Defendant would not utilize standard measures to reasonably secure her sensitive information.

232. Because of the Data Breach, Plaintiff Petrillo's Private Information is now in the hands of cybercriminals. Plaintiff Petrillo and all Class Members are now imminently at risk of crippling future identity theft and fraud.

233. As a result of the Data Breach, Plaintiff Petrillo has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, researching how best to ensure that she is protected from identity theft, reviewing account statements and other information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach.

234. Plaintiff Petrillo spent approximately three hours researching the data breach, freezing her credit, monitoring her accounts for suspicious activity, and changing her passwords. Plaintiff Petrillo continues to spend approximately an hour a week attempting to mitigate the consequences of the data breach.

235. Despite her efforts, Plaintiff Petrillo received notice that her information was exposed on the dark web.

236. Plaintiff Petrillo is very concerned and worried that her Private Information is now in the hand of cybercriminals.

237. Plaintiff Petrillo has also suffered injury directly and proximately caused by the Data Breach, including: (a) the theft of Plaintiff Petrillo's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Petrillo's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Petrillo's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of

the benefit of the bargain with Defendant to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff Petrillo should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Petrillo's Private Information; and (e) continued risk to Plaintiff Petrillo's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Stanley Williamson

238. Plaintiff Stanley Williamson is a former employee of HSG, having worked as Director of Environmental Sciences from November 2017 to March 2022. As a condition of his employment, Plaintiff Williamson was required to provide HSG with his sensitive Private Information, including his Social Security number, driver's license information, and direct deposit banking information.

239. On or about September 2, 2025, Plaintiff Williamson received a notice letter from HSG, dated August 25, 2025, informing him that his Private Information was compromised in the Data Breach.

240. As a direct and proximate result of the Data Breach, Plaintiff Williamson has already suffered actual injury. In August of 2025, prior to receiving the notice, he discovered fraudulent charges on his credit card. The account had to be closed, and cybercriminals continue to attempt to make charges on the closed account.

241. Plaintiff Williamson has also experienced an increase in spam phone calls since the Data Breach.

242. Plaintiff Williamson now faces an imminent, substantial, and ongoing risk of further identity theft and fraud. He has been forced to spend significant time dealing with the consequences of the Data Breach, including monitoring his financial accounts and credit reports, and will have to continue these mitigation efforts for the foreseeable future. This is valuable time he would have otherwise spent on his work, family, and other personal pursuits.

243. Plaintiff Williamson has spent approximately ten hours researching the Data Breach, monitoring his accounts, changing his passwords, and requesting replacement payment cards. Plaintiff Williamson continues to spend approximately half an hour each week attempting to mitigate the consequences of the data breach.

244. The Data Breach has caused Plaintiff Williamson to suffer significant anxiety, stress, and fear for his financial security and the integrity of his identity. He has suffered lost time, annoyance, interference, and inconvenience, and has a continuing interest in ensuring that his Private Information that remains in HSG's possession is protected from future breaches.

CLASS ALLEGATIONS

245. Plaintiffs bring 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 Private Information was compromised in the Data Breach disclosed by Healthcare Services Group, Inc., including all who are sent notice of the Data Breach.

246. In addition to the Nationwide Class, Plaintiff Stacy Petrillo seeks to represent the following state class:

New Jersey Class

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

247. In addition to the Nationwide Class, Plaintiff Rebecca Richards seeks to represent the following state class:

Washington Class

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

248. In addition to the Nationwide Class, Plaintiff Harold Henderson seeks to represent the following state class:

Texas Class

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

249. In addition to the Nationwide Class, Plaintiff Stanley Williamson seeks to represent the following state class:

Florida Class

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

250. 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).

251. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

252. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of Plaintiffs' 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.

253. **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' Private Information was exposed in the Data Breach. The Class Members are identifiable within Defendant's records because Defendant has their Private Information and has already reported that their Private Information was accessed from Defendant's systems.

254. **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 Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

b. Whether the computer systems and data security practices employed by HSG to protect Plaintiffs' and Class Members' Private 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 Plaintiffs and Class Members;

e. Whether Plaintiffs 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 Plaintiffs' and Class Members' Private 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 Plaintiffs and Class Members;

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

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

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

255. HSG engaged in a common course of conduct, giving rise to the legal rights sought to be enforced by Plaintiffs 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.

256. **Typicality**: Plaintiffs' claims are typical of the claims of the class. Plaintiffs, like all proposed members of the class, had Private Information compromised in the Data Breach. Plaintiffs and Class Members were injured by the same wrongful acts, practices, and omissions committed by HSG, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

257. **Adequacy**: Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs are adequate representatives of the class and have no interests adverse to, or in conflict with, the class that Plaintiffs seeks to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

258. **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 Plaintiffs and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against 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.

259. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure

to afford relief to Plaintiffs 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 Plaintiffs 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.

260. 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.

261. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

262. Unless a class-wide injunction is issued, HSG may continue in its failure to properly secure the Private 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.

263. 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 Plaintiffs and All Classes)

264. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

265. HSG collected the Private Information of Plaintiffs and Class Members in the ordinary course of employing or of providing services directly or indirectly to Plaintiffs and Class Members.

266. HSG owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting their Private 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.

267. HSG knew, or should have known, the risks of collecting and storing Plaintiffs' and Class Members' Private 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.

268. Given the nature of HSG's business, the sensitivity and value of the Private 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.

269. HSG breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private 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 Private Information entrusted to it—including Plaintiffs' and Class Members' Private Information.

270. Plaintiffs relied on Defendant to safeguard the Private Information entrusted to it and Defendant was in an exclusive position to protect against the foreseeable threat of a cyberattack.

271. It was reasonably foreseeable to HSG that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private 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 Plaintiffs' and Class Members' Private Information to unauthorized individuals.

272. HSG's duty of care to use reasonable security measures also arose as a result of the special relationships that existed between HSG and employees, and 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.

273. 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 Private Information.

274. But for HSG's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

275. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures

to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above (*see* ¶¶ 65-74, *supra*), together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendant's duty in this regard.

276. Pursuant to Section 5 of the FTCA, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

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

278. Specifically, Defendant breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

279. Defendant also violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein.

280. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendant's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

281. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect and Defendant's failure to comply with the FTCA constitutes negligence *per se*.

282. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Defendant's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

283. As a result of HSG's above-described negligent and wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs 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) the compromise, publication, improper disclosure, and theft of their Private Information; (iii) the breach of the confidentiality of their Private Information; (iv) damage to, diminution in, and deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (vi) lost time, money, and opportunity costs associated with effort attempting to mitigate and remediate the actual and future consequences of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; (vii) the continued risk to their Private Information, which remains in HSG's possession; (viii) actual or attempted fraud; (ix) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (x) the diminished value of HSG's services they received.

284. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

285. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs Richards, Henderson, and Williamson and All Classes)

286. Plaintiffs Richards, Henderson, and Williamson ("Plaintiffs" for the purposes of this Count) reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

287. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of receiving employment or services, directly or indirectly, from Defendant. Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's employment or services.

288. Plaintiffs and Class Members reasonably understood that a portion of the funds generated by their employment or payment for Defendant's services would be used to pay for adequate cybersecurity measures.

289. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

290. Plaintiff and the Class Members accepted Defendant's offers by disclosing their Private Information to Defendant in exchange for employment or services.

291. In turn, and through internal policies, Defendant agreed to protect and not disclose the Private Information to unauthorized persons.

292. In its Privacy Policy, Defendant represented that it had a legal duty to protect Plaintiffs' and Class Members' Private Information.

293. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

294. After all, Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of such an agreement with Defendant.

295. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

296. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

297. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

298. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic Private Information that Defendant created, received, maintained, and transmitted.

299. In these and other ways, Defendant violated its duty of good faith and fair dealing.

300. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

301. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

COUNT III
BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS WERE INTENDED THIRD-PARTY BENEFICIARIES
(On Behalf of Plaintiff Petrillo and the Nationwide Class)

302. Plaintiff Petrillo ("Plaintiff" for the purposes of this Count) realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

303. HSG had valid contracts with each of the nursing homes, retirement complexes, rehabilitation centers, hospitals, and other healthcare facilities to which it provided management, administrative, operating expertise, and other services. A principal purpose of those contracts was to securely store, transmit, and safeguard the Private Information of Plaintiff and Class Members.

304. Upon information and belief, HSG and each of the contracting nursing homes, retirement complexes, rehabilitation centers, hospitals, and other healthcare facilities expressed an intention that Plaintiff and Class Members were intended third-party beneficiaries of these agreements.

305. Plaintiff and Class Members are also intended third-party beneficiaries of these agreements because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances indicate that HSG intended to give the beneficiaries the benefit of the promised performance.

306. HSG breached its agreements with the contracting nursing homes, retirement complexes, rehabilitation centers, hospitals, and other healthcare facilities by allowing the data breach to occur, and as otherwise set forth herein.

307. HSG's breach caused foreseeable and material damages to Plaintiffs and Class Members (as detailed, *supra*).

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and All Classes)

308. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

309. Plaintiffs and Class Members either directly or indirectly gave HSG their Private Information in confidence, believing that HSG would protect that information. Plaintiffs 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 Plaintiffs' and Class Members' Private Information created a fiduciary relationship between HSG and Plaintiffs and Class Members. In

light of this relationship, HSG must act primarily for the benefit of Plaintiffs and Class Members, which includes safeguarding and protecting Plaintiffs' and Class Members' Private Information.

310. HSG accepted and used Plaintiffs' and Class Members' Private Information for its own pecuniary benefit and accepted the Private 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 Plaintiffs and Class Members if the confidentiality of their Private Information was breached.

311. HSG was in a superior position of trust and authority to Plaintiffs and Class Members.

312. Plaintiffs 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.

313. HSG has a fiduciary duty to act for the benefit of Plaintiffs 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 Plaintiffs' and Class Members' Private Information, failing to comply with the data security guidelines set forth by HIPAA and the FTCA, and otherwise failing to safeguard the Private Information of Plaintiffs 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.

314. As a direct and proximate result of HSG's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (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) the compromise,

publication, improper disclosure, and theft of their Private Information; (iii) the breach of the confidentiality of their Private Information; (iv) damage to, diminution in, and deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (vi) lost time, money, and opportunity costs associated with effort attempting to mitigate and remediate the actual and future consequences of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; (vii) the continued risk to their Private Information, which remains in HSG's possession; (viii) actual or attempted fraud; (ix) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (x) the diminished value of HSG's services they received.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and All Classes)

315. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

317. Plaintiffs and Class Members conferred a monetary benefit, directly or indirectly, upon HSG in the form of: (1) the revenues generated from Plaintiffs' and the classes' employment; (2) HSG using their Private Information to provide employment and facilitate its business operations; and/or (3) monies paid to receive HSG's services.

318. HSG accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. HSG also benefitted from the receipt of Plaintiffs' and Class Members' Private Information.

319. HSG unjustly enriched itself with regards to employee Plaintiffs and Class Members by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

320. HSG unjustly enriched itself with regard to Plaintiffs and Class Members in an amount equal to the difference in value between Plaintiffs' and Class Members' payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

321. Under principles of equity and good conscience, HSG should not be permitted to retain the full value of Plaintiffs' and Class Members' employment, and/or the full value of money belonging to Plaintiffs and Class Members, because HSG failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

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

323. HSG should be compelled to provide for the benefit of Plaintiffs and Class Members all unlawful proceeds received by it as a result of its misconduct and the Data Breach.

COUNT VI
VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT
N.J. Stat. Ann. § 56:8-2, *et seq.*
(On Behalf of Plaintiff Stacy Petrillo and the New Jersey Subclass)

324. Plaintiff Petrillo ("Plaintiff" for the purposes of this Count) realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

325. Plaintiff Stacy Petrillo brings this claim for relief individually and on behalf of the New Jersey Subclass pursuant to New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq*. ("NJCFA").

326. By engaging in the conduct alleged in this Complaint, HSG intended to and did engage in the sale of "merchandise" (which includes "services" under § 56:8-1) to consumers as defined by NJCFA.

327. HSG's relevant acts, practices and omissions complained of in this action were done in the course of HSG's business of providing management, administrative, operating expertise, and other services to the healthcare industry, including nursing homes, retirement complexes, rehabilitation centers, and hospitals throughout the State of New Jersey and the United States.

328. The NJCFA prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the State of New Jersey.

329. In the conduct of its business, trade, and commerce, and in the sale of management, administrative, operating expertise, and other services to the healthcare industry in the State of New Jersey, HSG collected and stored highly personal and private information, including sensitive PII and PHI of clients/patients and employees of HSG, like Plaintiff Stacy Petrillo and members of the putative Subclass.

330. HSG knew, or should have known, that its computer systems and data security practices were inadequate to safeguard the sensitive PII and PHI of Plaintiff Stacy Petrillo and the Subclass and that the risk of data breach was highly likely.

331. HSG should have disclosed this information regarding its computer systems and data security practices because HSG was in a superior position to know the true facts related to its

security vulnerability, and members of the Subclass could not reasonably be expected to learn or discover the true facts.

332. As alleged throughout this Complaint, HSG's deliberate conduct constitutes deceptive, unfair and unlawful trade acts or practices in the conduct of trade or commerce and the furnishing of services in the State of New Jersey, in violation of the NJCFA, including, but not limited to, its:

a. Failure to maintain adequate computer systems and data security practices to safeguard consumers' PII and PHI;

b. Failure to disclose that its computer systems and/or payment processor servers and data security practices were inadequate to safeguard consumers' PII and PHI from theft;

c. Misrepresenting the material fact that HSG would maintain adequate data, privacy and security practices and procedures to safeguard customer's PII and PHI from unauthorized disclosure, release, data breaches, and theft;

d. Failure to timely and accurately disclose the data breach to Plaintiff Stacy Petrillo and other members of the Subclass and knowingly omitting, suppressing, and concealing the material fact that HSG's computer systems and data security practices were inadequate to safeguard customers' PII and PHI from theft, with the intent that others rely upon the omission, suppression, and concealment;

e. Continued acceptance of PII and PHI and storage of other personal information after HSG knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach; and

f. Continued acceptance of PII and PHI and storage of other personal information after HSG knew or should have known of the Data Breach and before it allegedly remediated the Breach.

333. Plaintiff Stacy Petrillo and other members of the Subclass relied upon HSG's deceptive and unlawful conduct, and HSG's conduct was negligent, knowing and willful, and/or wanton and reckless with respect to the Subclass.

334. Plaintiff Stacy Petrillo and other members of the Subclass entrusted HSG with their PII and PHI.

335. As a direct and proximate result of HSG's violation of the NJCFA, members of the New Jersey Subclass 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 Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private 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 Private 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 Private 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 Plaintiffs and Class Members; and (ix) the diminished value of HSG's services they received.

336. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of HSG alleged herein, the Subclass seeks relief under N.J. Stat. Ann. § 56:8-19,

including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

337. Pursuant to N.J. Stat. Ann. § 56:8-20, this Complaint will be served upon the New Jersey Attorney General.

COUNT VII
VIOLATIONS OF THE WASHINGTON CONSUMER PROTECTION ACT RCW 19.86
(On Behalf of Plaintiff Rebecca Richards and the Washington Subclass)

338. Plaintiff Richards ("Plaintiff" for the purposes of this Count) realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

339. Plaintiff Rebecca Richards brings this claim for relief individually and on behalf of the Washington Subclass pursuant to Washington Consumer Protection Act, RCW 19.86 ("CPA").

340. By engaging in the conduct alleged in this Complaint, HSG intended to and did engage in trade and commerce as defined by the CPA.

341. HSG's relevant acts, practices and omissions complained of in this action were done in the course of HSG's business of providing management, administrative, operating expertise, and other services to the healthcare industry, including nursing homes, retirement complexes, rehabilitation centers, and hospitals throughout the State of Washington and the United States.

342. The CPA prohibits unfair or deceptive acts or practices in the conduct of any trade or commerce in the State of Washington.

343. In the conduct of its trade and commerce, and in the sale of management, administrative, operating expertise, and other services to the healthcare industry in the State of Washington, HSG collected and stored highly personal and private information, including sensitive

PII and PHI of clients/patients and employees of HSG, like Plaintiff Rebecca Richards and members of the putative Subclass.

344. HSG knew, or should have known, that its computer systems and data security practices were inadequate to safeguard the sensitive PII and PHI of Plaintiff Rebecca Richards and the Subclass and that the risk of data breach was highly likely.

345. HSG should have disclosed this information regarding its computer systems and data security practices because HSG was in a superior position to know the true facts related to its security vulnerability, and members of the Subclass could not reasonably be expected to learn or discover the true facts.

346. As alleged throughout this Complaint, HSG's deliberate conduct constitutes deceptive, unfair, and unlawful acts or practices in the conduct of trade and commerce in the State of Washington, in violation of the CPA, including, but not limited to, its:

a. Failure to maintain adequate computer systems and data security practices to safeguard consumers' PII and PHI;

b. Failure to disclose that its computer systems and/or payment processor servers and data security practices were inadequate to safeguard consumers' PII and PHI from theft;

c. Misrepresenting the material fact that HSG would maintain adequate data, privacy and security practices and procedures to safeguard customer's PII and PHI from unauthorized disclosure, release, data breaches, and theft;

d. Failure to timely and accurately disclose the data breach to Plaintiff Rebecca Richards and other members of the Subclass and knowingly omitting, suppressing, and concealing the material fact that HSG's computer systems

and data security practices were inadequate to safeguard customers' PII and PHI from theft, with the intent that others rely upon the omission, suppression, and concealment;

e. Continued acceptance of PII and PHI and storage of other personal information after HSG knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach; and

f. Continued acceptance of PII and PHI and storage of other personal information after HSG knew, or should have known, of the Data Breach and before it allegedly remediated the Breach.

347. Plaintiff Rebecca Richards and other members of the Subclass relied upon HSG's deceptive and unlawful conduct, and HSG's conduct was negligent, knowing and willful, and/or wanton and reckless with respect to the Subclass.

348. Plaintiff Rebecca Richards and other members of the Subclass entrusted HSG with their PII and PHI.

349. As a direct and proximate result of HSG's violation of the CPA, members of the Washington Subclass 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 Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private 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 Private 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 Private 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 Plaintiffs and Class Members; and (ix) the diminished value of HSG's services they received.

350. Pursuant to RCW 19.86.093(3), Plaintiff alleges that HSG's conduct is injurious to the public interest because it injured, and had/has the capacity to injure, other persons.

351. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of HSG alleged herein, the Subclass seeks relief under RCW 19.86.090, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

COUNT VIII
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and All Classes)

352. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

354. HSG owes a duty of care to Plaintiffs and Class Members that require it to adequately secure Plaintiffs' and Class Members' Private Information.

355. HSG still possesses the Private Information of Plaintiffs and Class Members.

356. HSG has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members.

357. 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 Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and HSG's failure to address the security failings that led to such

exposure.

358. 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.

359. Plaintiffs, 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 Private Information not necessary for its provision of services;

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

h. Prohibiting HSG from maintaining the Private Information of Plaintiffs 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 Private Information, including, but not limited to, patient PII and patient PHI;

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 ten 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; and

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

PRAYER FOR RELIEF

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

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

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

C. Awarding Plaintiffs and the classes equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, 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 Private 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 Plaintiffs and the classes pre-judgment and post-judgment interest to the maximum extent allowable;

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

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: December 19, 2025

Respectfully submitted,

/s/ Benjamin F. Johns
Benjamin F. Johns (PA ID 201373)
Samantha E. Holbrook (PA ID 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

Andrew W. Ferich (PA ID 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

Charles E. Schaffer (PA ID 76259)
LEVIN SEDRAN & BERMAN LLP
510 Walnut St, Suite 500
Philadelphia, PA 19106
T.: (215) 592-1500
cschaffer@lfsblaw.com

Mariya Weekes (*pro hac vice* forthcoming)
MILBERG, PLLC
333 SE 2nd Avenue, Suite 2000
Miami, FL 33131
Tel: (866) 252-0878
mweekes@milberg.com

Kenneth J. Grunfeld
Courtney Maccarone (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW P.A.
65 Overhill Road
Bala Cynwyd, PA 19004
Telephone: (954) 525-4100
grunfeld@kolawyers.com
maccarone@kolawyers.com

Leanna A. Loginov (*pro hac vice* forthcoming)
SHAMIS & GENTILE, P.A.
14 NE 1st Ave, Suite 705
Miami, FL 33132
Telephone: (305) 479-2299
lloginov@shamisgentile.com

Nicholas Sandercock (PA ID 324421)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel: (212) 532-1091
nsandercock@sirillp.com
tbean@sirillp.com

A. Brooke Murphy (*pro hac vice* to be filed)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Tel: (405) 389-4989
abm@murphylegalfirm.com

Nicholas Sandercock (PA ID 324421)
Tyler J. Bean (pro hac vice to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel: (212) 532-1091
nsandercock@sirillp.com
tbean@sirillp.com

Mark S. Reich (*pro hac vice* forthcoming)
Melissa G. Meyer (*pro hac vice* forthcoming)
LEVI & KORSINSKY, LLP
33 Whitehall Street, 27th Floor

New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: mmeyer@zlk.com

Daniel Srourian, Esq. (*pro hac vice* forthcoming)
SROURIAN LAW FIRM, P.C.
468 N. Camden Drive, Suite 200
Beverly Hills, CA 90210
Tel: (213) 474-3800
daniel@slfla.com

Gregory Haroutunian (*pro hac vice*)
EMERY REDDY, PC
600 Stewart Street, Suite 1100
Seattle, WA 98101
Tel: (916) 823-6955
gregory@emeryreddy.com

Ben Barnow (*pro hac vice* forthcoming)
Anthony L. Parkhill (*pro hac vice* forthcoming)
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com

Leigh S. Montgomery
EKSM, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Tel: (888) 350-3931
Fax: (888) 276-3455
service@eksm.com

Jonathan S. Mann (admitted *pro hac vice*)
PITTMAN, DUTTMAN, HELLUMS, BRADLEY & MANN, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
Fax: (205) 328-2711
jonm@pittmandutton.com

Zachary Arbitman
George A. Donnelly
FELDMAN SHEPHERD WOHLGELERNTER TANNER WEINSTOCK & DODIG, LLP
1845 Walnut Street, 21st Floor
Philadelphia, PA 19103
Tel: (215) 567-8300
zarbitman@feldmanshepherd.com
gdonnelly@feldmamshepherd.com

Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I, Benjamin F. Johns, hereby certify that on this 19th day of December 2025, I caused the foregoing Consolidated Class Action Complaint to be filed using the Court's CM/ECF system, thereby causing it to be electronically served upon all counsel of record in this matter.

/s/ Benjamin F. Johns
Benjamin F. Johns