Exhibit A2

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

Michael Rentschler, Cathy Ehrisman, Heather Byam, and Kathleen Appel, individually, and on behalf of all others similarly situated, Plaintiffs, v. Atlantic General Hospital Corporation. Defendant.	Case No. 1:23-cv-01005 Hon. Julie R. Rubin

SECOND CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Michael Rentschler, Cathy Ehrisman, Heather Byam, and Kathleen Appel ("Plaintiffs"), individually, and on behalf of all others similarly situated, bring this action against Atlantic General Hospital Corporation, ("AGH" or "Defendant"), by and through their attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information and belief as to all other matters, as follows.

I. INTRODUCTION

1. Atlantic General Hospital Corporation runs multiple hospitals and other health care services throughout the State of Maryland.

2. As a comprehensive healthcare services company, AGH collects, maintains, and stores highly sensitive personal and medical information pertaining to its patients, including, but not limited to: Social Security numbers, dates of birth, full names, addresses, telephone numbers, and driver's license numbers ("personally identifying information" or "PII"), as well as information regarding medical treatment, diagnosis, and prescriptions, medical record numbers, health insurance information, other protected health information ("private health information" or

"PHI"), as well as financial account/payment card information ("financial account information" and, collectively with PII and PHI, "Private Information").

3. Although AGH is a sophisticated healthcare company, it failed to invest in adequate data security, and as a direct, proximate, and foreseeable result of its inexcusable failure to implement reasonable security protections sufficient to prevent an eminently avoidable cyberattack, unauthorized actors compromised its company networks and accessed patients' files containing highly-sensitive Private Information.

4. According to the data breach notice that AGH sent to affected individuals, AGH discovered suspicious activity in its company networks on January 29, 2023, and began an investigation with the aid of a third-party forensic specialists. The investigation determined that infiltrators breached AGH servers beginning on January 20, 2023, and had accessed numerous files.

5. On March 6, 2023, AGH's investigation determined that the unauthorized actor(s) accessed files that contained sensitive information that could identify current and former AGH patients. The Private Information exposed by the breach included names, social security numbers, driver's license numbers, financial account information, dates of birth, medical record numbers, physician information, health insurance information, subscriber numbers, medical history information, and diagnosis/treatment information.

6. On March 24, 2023, AGH issued a data breach notice to individuals that AGH believed had been affected by the breach. At that time, AGH estimated that approximately 30,704 individuals had been affected by the Data Breach.[1]

[1] Richard Console, Jr., *Atlantic General Hospital Notifies 30,704 Patients of Recent Data Breach Affecting Their SSNs and PHI*, JDSupra (March 27, 2023), available at: https://www.jdsupra.com/legalnews/atlantic-general-hospital-notifies-30-2202615/.

7. As AGH continued to investigate the Data Breach, it determined that an additional one-hundred-thousand (100,000) individuals were impacted by the Data Breach. Now, AGH estimates the number of affected individuals to be at least 136,981.[2] AGH issued data breach notifications to these individuals on June 22, 2023.

8. AGH's failure to promptly notify Plaintiffs and Class members that their Private Information was exfiltrated due to AGH's apparent security failures virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse and/or disseminate that Private Information before Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

9. It is clear that AGH failed to take sufficient and reasonable measures to safeguard its data security systems and protect highly sensitive data in order to prevent the Data Breach from occurring; to disclose to its patients, and the public at large, that it lacked appropriate data systems and security practices to secure Private Information; and to timely detect and provide adequate notice of the Data Breach to affected individuals.

10. As a result of AGH's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs' and Class members' Private Information was accessed and acquired by unauthorized third-parties for the

[2] *Data Breach Notification – Atlantic General Hospital*, Office of the Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/dd9e509f-bdbf-49ba-abae-56239ec46b6b.shtml; Steve Adler, *Atlantic General Hospital Increases Ransomware Victim Count to Almost 140,000 Individuals*, The HIPAA Journal (June 27, 2023), available at https://www.hipaajournal.com/atlantic-general-hospital-increases-ransomware-victim-count-to-almost-140000-individuals/.

express purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of AGH's patients. Plaintiffs and Class members face the real, immediate, and likely danger of identity theft and misuse of their Private Information, especially because their Private Information was specifically targeted by malevolent actors.

11. Plaintiffs and Class members suffered injuries as a result of AGH's conduct including, but not limited to: lost or diminished value of their Private Information; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change usernames and passwords on their accounts; time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their Private Information, which remains in AGH's possession and is subject to further unauthorized disclosures so long as AGH fails to undertake appropriate and adequate measures to protect their Private Information. These risks will remain for the lifetimes of Plaintiffs and the Class.

12. Accordingly, Plaintiffs bring this action on behalf of all those similarly situated to seek relief from Defendant's failure to reasonably safeguard Plaintiffs' and Class members' Private Information; its failure to reasonably provide timely notification that Plaintiffs' and Class members' Private Information had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiffs and Class members concerning the status, safety, location, access, and protection of their Private Information.

II. PARTIES

Plaintiff Michael Rentschler

13. Plaintiff Michael Rentschler is a resident and citizen of Maryland. Plaintiff Rentschler is a patient of AGH and has been for approximately 51 years. Plaintiff Rentschler received AGH's Data Breach Notice by U.S. mail in or about March 2023.

Plaintiff Cathy Ehrisman

14. Plaintiff Cathy Ehrisman is a resident and citizen of Berwyn, Maryland. Plaintiff Ehrisman is a patient of AGH and has been for approximately ten years. Plaintiff Ehrisman received AGH's Data Breach Notice by U.S. mail in or about March 2023.

Plaintiff Heather Byam

15. Plaintiff Heather Byam is a resident and citizen of Maryland. Plaintiff Byam is a patient of AGH. Plaintiff Byam received AGH's Data Breach Notice via U.S. Mail in or about March of 2023.

Plaintiff Kathleen Appel

16. Plaintiff Kathleen Appel is a resident and citizen of Catonsville, Maryland. Plaintiff Appel is a patient of AGH. Plaintiff Appel received AGH's Data Breach Notice via U.S. Mail in or about March of 2023.

Defendant Atlantic General Hospital Corporation

17. Defendant Atlantic General Hospital is a Maryland Corporation with its principal place of business located at 9733 Healthway Drive, Berlin, MD 21811. Atlantic General Hospital Corporation runs over thirty hospitals and other health care service locations throughout Maryland, serving patients in Worcester, Wicomico, Somerset and Sussex Counties with a wide range of

general and specialty healthcare services. The Atlantic General Hospital Corporation employs more than 940 people and generates approximately $138 million in annual revenue.[3]

III. JURISDICTION AND VENUE

18. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

19. This Court has personal jurisdiction over Defendant because Defendant is headquartered in Maryland.

20. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' and Class members' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Atlantic General Hospital – Background

21. As part of its hospital and healthcare operations, AGH collects, maintains, and stores the highly sensitive PII and medical information provided by its current and former patients, including but not limited to: full names, addresses, Social Security numbers, dates of birth, medical and treatment information, health insurance information, driver's license numbers, passport information, financial account information and contact information.

[3] *Id.*

22. On information and belief, at the time of the Data Breach, AGH had failed to implement necessary data security safeguards, which resulted in unauthorized third parties accessing the Private Information of approximately 136,981 current and former patients.[4]

23. Current and former patients of AGH, such as Plaintiffs and Class members, allowed their Private Information to be made available with the reasonable expectation that any entity with access to this information would comply with its obligations to keep that sensitive and personal information confidential and secure from illegal and unauthorized access, and that those entities would provide them with prompt and accurate notice of any unauthorized access to their Private Information.

24. Unfortunately for Plaintiffs and Class members, AGH failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security, thus failing to protect Plaintiffs and Class members from having their Private Information exfiltrated during the Data Breach.

B. The Data Breach

25. On January 29, 2023, AGH discovered suspicious files on its company networks and launched an investigation to ascertain the nature of these files through the aid of third-party data forensics specialists.

26. This investigation revealed that intruders had breached AGH's systems on or about January 20, 2023, and accessed numerous files on its servers. AGH began an investigation to determine the types of information that had been stolen and the identity of those to whom the stolen

[4] *Data Breach Notification – Atlantic General Hospital*, Office of the Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/dd9e509f-bdbf-49ba-abae-56239ec46b6b.shtml.

information belonged, which took until March 6, 2023—more than one month after AGH discovered suspicious activity on its servers.[5]

27. On March 24, 2023, two weeks after AGH determined that Private Information concerning current and former patients had been accessed by unauthorized actors, and approximately two months after AGH discovered the suspicious activity on its serves, AGH finally informed the public about the Data Breach and sent notices to patients and other parties whose highly sensitive information had been stolen by the hackers.[6] AGH estimated that 30,704 individuals were affected by the breach.

28. AGH then began a more thorough investigation, which was not completed until approximately May 15, 2023. This investigation determined that over 100,000 additional individuals were affected by the breach with a new estimated total of 136,981 affected individuals.[7] Thereafter, on June 22, 2023, AGH issued a data breach notice to these second tranche of affected individuals.

29. Between the alleged date of discovery on January 29, 2023, and March 24, 2023, when AGH issued its data breach notice to the first tranche of 30,704 affected individuals, 54-days had elapsed. Moreover, between the alleged date of discovery on January 29, 2023, and June 22, 203, when AGH issued its second round of notices to the 106,277 affected additional individuals, 144 days had elapsed.

---

[5] *Id.*
[6] *Id.*
[7] *Data Breach Notification – Atlantic General Hospital*, Office of the Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/dd9e509f-bdbf-49ba-abae-56239ec46b6b.shtml.

C. AGH's Many Failures Both Prior to and Following the Breach

30. AGH could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and network files containing Private Information.

31. To be sure, collecting, maintaining, and protecting Private Information is vital to virtually every aspect of AGH's operation as a hospital and healthcare service provider. Yet, AGH failed to detect that its own data system had been compromised until more than a week after the intruders breached its networks.[8]

32. When AGH finally acknowledged that it had experienced a breach, it failed to fully inform affected individuals of the length of time that the unauthorized actors had access to Plaintiffs' and Class members' Private Information, or the full extent of the Private Information that was accessed during the Data Breach. AGH did, however, acknowledge that in response to the cyber-attack it began "taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security,"[9] implicitly admitting that its information systems policies and protocols were inadequate prior to the Data Breach.

33. AGH's failure to properly safeguard Plaintiffs' and Class members' Private Information allowed the unauthorized actors to access this highly valuable information, but AGH's failure to timely notify Plaintiffs and other victims of the Data Breach that their Private Information had been misappropriated served only to exacerbate the harms they suffered as a direct and proximate result thereof, because it precluded them from taking meaningful steps to safeguard their identities prior to the further dissemination and misuse of their Private Information.

[8] *Id.*
[9] *Id.*

34. First, AGH failed to timely discover the Data Breach and immediately secure its computer systems to protect its current and former patients' Private Information. It instead allowed unauthorized actors unfettered access to its computer systems for approximately nine days before discovering the breach.

35. Second, AGH failed to timely notify affected individuals, including Plaintiffs and Class members, that their highly-sensitive Private Information had been accessed by unauthorized third parties. Of the 136,981 affected individuals, 30,704 individuals were not notified of the breach until 54-days after AGH allegedly discovered the breach and 106,277 were not notified until 144-days after the breach was discovered.

36. Third, AGH has made no effort to protect Plaintiffs and the Class from the long-term consequences of AGH's acts and omissions. Although the notice offered victims a complimentary one-year access to IDX credit monitoring, Plaintiffs' and Class members' PII, including their Social Security numbers, and even more immutable PHI cannot be changed and will remain at risk long beyond one year. As a result, Plaintiffs and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

37. In short, AGH's myriad failures, including the failure to timely detect the Data Breach and/or notify Plaintiffs and Class members that their personal and medical information had been exfiltrated due to AGH's security failures, allowed unauthorized individuals to access, misappropriate and misuse Plaintiffs' and Class members' Private Information for *months* before AGH finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

38. Data breaches have become a constant threat, and the PII exfiltrated during such an attack, including Social Security numbers in particular, are a particularly valuable commodity and a frequent target of hackers.

39. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[10] The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just 8 shy of the record of 715 set in 2021 and still double that of the number of similar such compromises in 2017 and triple the number of compromises in 2012.[11]

40. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[12] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%. [13]

---

[10] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report.

[11] *2022 Healthcare Data Breach Report*, The HIPAA Journal (January 24, 2023), available at: https://www.hipaajournal.com/2022-healthcare-data-breach-report/.

[12] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista, available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[13] *Id.*

41. Data breaches are a constant threat because PII is routinely traded on the dark web as a simple commodity, with social security numbers being so ubiquitous to be sold at as little as $2.99 apiece and passports retailing for as little as $15 apiece.[14]

42. In addition, the severity of the consequences of a compromised social security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory elements can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [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, 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.[15]

43. This is exacerbated by the fact that the problems arising from a compromised social security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[16]

---

[14] *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.

[15] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[16] *Id.*

44. Beyond social security numbers, the most sought after and expensive PII on the dark web are stolen medical records, which command prices from $250 to $1,000 each.[17] Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and social security numbers, which can be changed, medical records contain "a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[18] With this bounty of ill-gotten information, cybercriminals can wreak havoc and perpetuate serious crimes such as drug dealing (by obtaining prescriptions under the victims' names) and major fraud (by filing large-scale and bogus insurance claims).[19]

45. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of $13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (by contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[20] It is also "considerably harder" to reverse the damage from medical identity theft with victims routinely suffering long term harassment from aggressive medical debt collection practices, irreversible damage to credit, and even prosecution after thieves used their stolen data to purchase drugs for the illegal drug trade.[21]

---

[17] Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (January 26, 2021), available at: https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

[18] *Id.*

[19] *Id.*

[20] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.

[21] *Id.*

46. Instances of Medical identity theft have grown exponentially over the years from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.[22]

47. As explained by Kunal Rupani, director of product management at Accellion, a private cloud solutions company, in the context of a different medical data breach:

> Unlike credit card numbers and other financial data, healthcare information doesn't have an expiration date. As a result, a patient's records can sell on the black market for upwards of fifty times the amount of their credit card number, making hospitals and other healthcare organizations extremely lucrative targets for cybercriminals.[23]

48. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendant charged with maintaining and securing patient PII know the importance of protecting that information from unauthorized disclosure. Indeed, on information and belief, Defendant was aware of highly publicized security breaches where PII and protected health information was accessed by unauthorized cybercriminals, including breaches of computer systems involving: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[24]

49. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized

---

[22] *Id.*

[23] Jeff Goldman, 21st Century Oncology Notifies 2.2 Million Patients of Data Breach (Mar. 11, 2016), http://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html.

[24] *See e.g.*, *Healthcare Data Breach Statistics*, HIPAA Journal, available at: https://www.hipaajournal.com/healthcare-data-breach-statistics.

these enforcement actions to place companies like Defendant on notice of their obligation to safeguard customer and patient information.

50. Indeed, 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 take appropriate measures to prepare for and are able to thwart such an attack.

51. Given the nature of AGH's Data Breach, as well as the length of the time AGH's networks were breached and the long delay in notification to the Class, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class members' Private Information can easily obtain Plaintiffs' and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

52. 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 credit card victims can cancel or close credit and debit card accounts.[25] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

53. To date, AGH has offered its consumers *only one year* of identity theft monitoring services. The offered services are inadequate to protect Plaintiffs and the Class from the threats they will face for years to come, particularly in light of the Private Information at issue here.

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

54. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, AGH failed to take appropriate steps to protect the Private Information of Plaintiffs and the Class from misappropriation. As a result, the injuries to Plaintiffs and the Class were directly and proximately caused by AGH's failure to implement or maintain adequate data security measures for its current and former patients.

E. AGH Had a Duty and Obligation to Protect Private Information

55. AGH has an obligation, both statutory and self-imposed, to keep confidential and protect from unauthorized access and/or disclosure Plaintiffs' and Class members' Private Information. AGH's obligations are derived from: 1) government regulations and state laws, including HIPAA and FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII and medical records. Plaintiffs and Class members provided, and AGH obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

56. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

57. Additionally, HIPAA requires Covered Entities and Business Associates to provide notification to every affected individual following the impermissible use or disclosures of any protected health information. The individual notice must be provided to affected individuals without unreasonable delay and no later than 60 days following discovery of the breach. Further, for a breach involving more than 500 individuals, entities are required to provide notice in prominent media outlets. *See* 45 CFR § 164.400, *et seq.*

58. Defendant has an obligation to comply with HIPAA requirements concerning the protection of PII and protected health information and prompt and adequate notification of data breaches.

59. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

60. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[26] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[27]

[26] 17 C.F.R. § 248.201 (2013).
[27] *Id.*

61. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-marking.[28]

62. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[29] The guidelines note 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 security problems.[30] 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.[31] AGH clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

63. Here, at all relevant times, AGH was fully aware of its obligation to protect the Private Information of its current and former patients, including Plaintiffs and the Class, and on information and belief, AGH is a sophisticated and technologically savvy hospital that relies extensively on technology systems and networks to maintain its practice, including storing its

[28] *Start With Security*, Federal Trade Commission (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[29] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.
[30] *Id.*
[31] *Id.*

patients' PII, protected health information, and medical information in order to operate its business.

64. AGH had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between AGH and Plaintiffs and Class members. AGH alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiffs' and Class members' Private Information.

65. AGH's failure to follow the FTC guidelines and its subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data constitutes unfair acts or practices prohibited by Section 5 of the Federal Trade Commission Act, 14 U.S.C. § 45.

66. Further, AGH had a duty to promptly notify Plaintiffs and the Class that their Private Information was accessed by unauthorized persons.

67. AGH was on notice that healthcare entities are particularly susceptible targets for data breaches.

68. The American Medical Association ("AMA") has 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.[32]

[32] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on July 18, 2023).

69. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[33] In 2022, the largest growth in compromises occurred in the healthcare sector.[34]

70. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[35]

71. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of victims were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[36]

72. As a healthcare provider, AGH knew, or should have known, the importance of safeguarding its patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences in the event this data was misappropriated. These consequences include the significant costs that would be imposed on AGH's patients as a result of a breach. AGH failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

---

[33] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on July 18, 2023).
[34] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on July 18, 2023).
[35] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on July 18, 2023).
[36] *Id*.

F. AGH Failed to Comply with HIPAA, FTC, and Industry Standard Data Protection Protocols

73. HIPAA obligates Covered Entities and Business Associates to adopt administrative, physical, and technology safeguards to ensure the confidentially, integrity, and security of consumer and patient PII and PHI.

74. The FTC rules, regulations, and guidelines obligate businesses to protect PII and PHI, from unauthorized access or disclosure by unauthorized persons.

75. At all relevant times, AGH was fully aware of its obligation to protect the patient PII and PHI entrusted to it by both Class members and AGH's patients, because it is a sophisticated business entity that is in the business of maintaining and transmitting PII and PHI.

76. AGH was also aware of the significant consequences of its failure to protect Private Information for the thousands of patients who provided their PII and medical information and knew that this data, if hacked, would gravely injure consumers, including Plaintiffs and Class members.

77. Unfortunately, AGH failed to comply with HIPAA, FTC rules, regulations and guidelines, and industry standards concerning the protection and security of Private Information. As evidenced by the duration, scope, and nature of the Data Breach, among its many deficient practices, AGH security failures also include, but are not limited to:

a. Failing to develop and employ adequate intrusion detection systems;

b. Failing to engage in regular reviews of audit logs and authentication records;

c. Failing to develop and maintain adequate data security systems to reduce the risk of data breaches and cyberattacks;

d. Failing to ensure the confidentiality and integrity of current and former patients' PII and protected health and information and records that Defendant receives and maintains;

e. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of its current and former patients' Private Information;

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

g. Failing to develop adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;

h. Failing to implement technical policies, procedures and safeguards for electronically stored information concerning Private Information that permit access for only those persons or programs that have specifically been granted access; and

i. Other similar measures to protect the security and confidentiality of its current and former patients' Private Information.

78. Had AGH implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. AGH could have prevented or detected the Data Breach prior to the hackers accessing AGH's systems and extracting sensitive and personal information; the amount and/or types of Private Information accessed by the hackers could have been avoided or greatly reduced; and current and former patients of AGH would have been notified sooner, allowing them to promptly take protective and mitigating actions.

G. AGH's Data Security Practices are Inadequate and Inconsistent with Industry Standards

79. AGH purports to care about data security and safeguarding patients' Private Information, and represents that it will keep secure and confidential the Private Information belonging to its current and former patients.[37]

[37] *Atlantic Genera Hospital Privacy Policy*, Atlantic General Hospital, available at https://www.atlanticgeneral.org/patients-visitors/privacy-policy/.

80. Plaintiffs and Class members provided their Private Information to AGH in reliance on its promises and self-imposed obligations to keep PII and medical information confidential, and to secure the Private Information from unauthorized access by malevolent actors. It failed to do so.

81. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

82. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

83. 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; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

84. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

86. Had AGH undertaken the actions that federal and state law require, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as AGH would have detected the Data Breach prior to the hackers extracting data from AGH's networks, and AGH's current and former patients would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

87. Indeed, following the Data Breach, AGH effectively conceded that its security practices were inadequate and ineffective. In the Notice it sent to Plaintiffs and others, AGH acknowledged that the Data Breach required it to add "additional safeguards."

H. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach

88. Like any data hack, the Data Breach presents major problems for all affected.[38]

89. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account,

[38] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.

run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[39]

90. The ramifications of AGH's failure to secure properly Plaintiffs' and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

91. According to data security experts, one out of every four data breach notification recipients becomes a victim of identity fraud.

92. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

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

94. 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

[39] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

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

95. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[40]

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

97. 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 Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

98. The existence and prevalence of "Fullz" packages means that the Private

[40] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

99. Thus, even if certain information (such as Social Security numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

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

101. Accordingly, AGH's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[41] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[42] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[43] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

102. The theft of medical information, beyond the theft of more traditional forms off PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far

---

[41] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), available at http://www.iii.org/insuranceindustryblog/?p=267.

[42] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), available at http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.

[43] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, available at https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf).

outstrips the increase in incidence of traditional identity theft.[44] Medical Identity Theft is especially nasty for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at $50), the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, $13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[45]

103. PII and PHI are valuable property rights.[46] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

104. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[47]

105. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[48]

106. Consumers who agree to provide their web browsing history to the Nielsen

[44] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.
[45] *Id.*
[46] *See, e.g.*, Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[47] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[48] *World Data Exchange*, World Data Exchange, available at: https://worlddataexchange.com.

Corporation can receive up to $50.00 a year.[49]

107. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[50]

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

109. In response to the Data Breach, AGH offered to provide certain individuals whose Private Information was exposed in the Data Breach with one year of credit monitoring. However, even one year of complimentary credit monitoring is a period much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiffs and Class members by AGH's failures.

110. Moreover, the credit monitoring offered by AGH is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Private Information.

111. Here, due to the Breach, Plaintiffs and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

[49] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[50] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite AGH's delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiffs' and Class members' privacy.

112. Plaintiffs and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will not abate within a mere one to two years: the unauthorized access of Plaintiffs' and Class members' Private Information, especially their Social Security numbers, puts Plaintiffs and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that AGH offered victims of the Breach. The one year of credit monitoring that AGH offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiffs and Class members have suffered and will continue to suffer as a result of the Data Breach.

113. As a direct and proximate result of AGH's acts and omissions in failing to protect and secure Private Information, Plaintiffs and Class members have been placed at a substantial

risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

114. Plaintiffs retain an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

PLAINTIFFS' EXPERIENCES

Michael Rentschler

115. Plaintiff Rentschler received AGH's Data Breach notice dated March 24, 2023. The notice informed him that his information had been improperly accessed and/or obtained by third parties. This notice indicated that his Private Information, including his name, address, telephone number, date of birth, Social Security number, driver's license number, health insurance information, treatment information, health information, and other financial information was compromised in the Data Breach.

116. As a result of the Data Breach, Plaintiff Rentschler has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Rentschler has spent several hours dealing with the Data Breach, valuable time Plaintiff Rentschler otherwise would have spent on other activities, including, but not limited to, work and recreation.

117. As a result of the Data Breach, Plaintiff Rentschler has suffered anxiety due to the public dissemination of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his Private Information for purposes of identity theft and fraud. Plaintiff Rentschler is concerned about

identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

118. Plaintiff Rentschler suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

119. As a result of the Data Breach, Plaintiff Rentschler anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Rentschler is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Cathy Ehrisman

120. Plaintiff Ehrisman received the Data Breach notice directly from Defendant, by U.S. mail, dated March 24, 2023. The notice informed her that her information had been improperly accessed and/or obtained by third parties. This notice indicated that her Private Information, including her name, address, telephone number, date of birth, Social Security number, driver's license number, health insurance information, treatment information, health information, and other financial information was compromised in the Data Breach.

121. As a result of the Data Breach, Plaintiff Ehrisman has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: changing passwords and re-securing her own computer network, signing up for credit monitoring and identity theft insurance, contacting credit bureaus to place freezes on her accounts, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud, which

may take years to detect. Plaintiff Ehrisman has spent significant time—at least several hours thus far—dealing with the Data Breach, valuable time Plaintiff Ehrisman otherwise would have spent on other activities, including, but not limited to, work and recreation.

122. As a result of the Data Breach, Plaintiff Ehrisman has suffered anxiety due to the public dissemination of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff Ehrisman is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

123. Plaintiff Ehrisman suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) fraudulent charges to her Amazon account—totaling more than $1000—that occurred between approximately December 2022 to June 2023; (ii) her Private Information being disseminated on the Dark Web, according to Experian; (iii) out-of-pocket costs spent on credit monitoring an identity theft insurance; (iv) an increase in spam calls, texts, and/or email; (v) invasion of privacy; (vi) loss of benefit of the bargain; (vii) lost time spent on activities remedying harms resulting from the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect her Private Information.

124. As a result of the Data Breach and the fraudulent charges made on her account, Plaintiff Ehrisman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Ehrisman is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Heather Byam

125. Plaintiff Byam received the Data Breach notice directly from Defendant, by U.S. mail, dated March 24, 2023. The notice informed her that her information had been improperly accessed and/or obtained by third parties. This notice indicated that her Private Information, including her name, address, telephone number, date of birth, Social Security number, driver's license number, health insurance information, treatment information, health information, and other financial information was compromised in the Data Breach.

126. As a result of the Data Breach, Plaintiff Byam has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: changing passwords and re-securing her own computer network, signing up for credit monitoring and identity theft insurance, contacting credit bureaus to place freezes on her accounts, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud, which may take years to detect. Plaintiff Byam has spent significant time—at least several hours thus far—dealing with the Data Breach, valuable time Plaintiff Byam otherwise would have spent on other activities, including, but not limited to, work and recreation.

127. In May 2023, Plaintiff Byam received notification of an unauthorized attempt to complete fraudulent transactions using her Victoria's Secret credit card. Additionally, after receiving the Data Breach Notice, Plaintiff Byam discovered that unauthorized individuals had

attempted to access her Amazon account in order to complete transactions using her Amazon credit card. Plaintiff Byam had to expend time, energy, and resources disputing the transactions, placing freezes on her credit, and closing and re-opening accounts at her financial institution.

128. As a result of the Data Breach and the attempted fraud she experienced, Plaintiff Byam has suffered anxiety due to the public dissemination of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff Byam is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

129. Plaintiff Byam suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

130. As a result of the Data Breach, Plaintiff Byam anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Byam is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Kathleen Appel

131. Plaintiff Appel received the Data Breach notice directly from Defendant, by U.S. mail, dated March 24, 2023. The notice informed her that her information had been improperly accessed and/or obtained by third parties. This notice indicated that her Private Information, including her name, address, telephone number, date of birth, Social Security number, driver's

license number, health insurance information, treatment information, health information, and other financial information was compromised in the Data Breach.

132. As a result of the Data Breach, Plaintiff Appel has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: changing passwords and re-securing her own computer network, signing up for credit monitoring and identity theft insurance, contacting credit bureaus to place freezes on her accounts, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud, which may take years to detect. Plaintiff Appel has spent significant time—at least several hours thus far—dealing with the Data Breach, valuable time Plaintiff Appel otherwise would have spent on other activities, including, but not limited to, work and recreation.

133. In May 2023, Medicare informed Plaintiff Appel that her Medicare and supplemental health insurance information were used to claim and obtain $15,920 worth of medical services in New York. Plaintiff Appel never sought or received medical services in New York state and she determined that her information had been used fraudulently. Plaintiff Appel immediately contacted Medicare to report the fraud. Plaintiff Appel and her husband spent several hours investigating this fraud, reporting the fraud, and attempting to mitigate the fraud.

134. As a result of the Data Breach and the serious Medicare fraud perpetrated using her stolen information, Plaintiff Appel has suffered anxiety due to the public dissemination of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff Appel is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

135. Plaintiff Appel suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

136. As a result of the Data Breach, Plaintiff Appel anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Appel is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

137. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose Private Information was accessed in the Data Breach, including all those who received a Notice Letter.

Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change or expand the Class definition after conducting discovery.

138. In the alternative, Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

> All persons who are residents of the State of Maryland whose Private Information was accessed in the Data Breach, including all those who received a Notice Letter (the "Maryland Subclass").

Excluded from the Maryland Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

139. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable with the number of affected individuals estimated to be 136,981.[51] The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of AGH and obtainable by Plaintiffs only through the discovery process. The members of the Class will be identifiable through information and records in AGH's possession, custody, and control.

140. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether AGH's data security and retention policies were unreasonable;

b. Whether AGH failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether AGH owed a duty to Plaintiffs and Class members to safeguard their Private Information;

d. Whether AGH breached any legal duties in connection with the Data Breach;

e. Whether AGH's conduct was intentional, reckless, willful or negligent;

f. Whether an implied contract was created concerning the security of Plaintiffs' and Class members' Private Information;

g. Whether AGH breached that implied contract by failing to protect and keep secure Plaintiffs' and Class members' Private Information and/or failing to timely and adequately notify Plaintiffs and Class members of the Data Breach;

h. Whether Plaintiffs and Class members suffered damages as a result of AGH's conduct; and

[51] *Data Breach Notification – Atlantic General Hospital*, Office of the Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/dd9e509f-bdbf-49ba-abae-56239ec46b6b.shtml.

i. Whether Plaintiffs and the Class are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

141. Typicality: All of Plaintiffs' claims are typical of the claims of the Class since Plaintiffs and all members of the Class had their Private Information compromised in the Data Breach. Plaintiffs and the members of the Class sustained damages as a result of AGH's uniform wrongful conduct.

142. Adequacy: Plaintiffs are adequate representatives because their interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, they have retained counsel competent and highly experienced in complex class action litigation, and intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor their counsel have any interests that are antagonistic to the interests of other members of the Class.

143. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by AGH's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. 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. Members of the Class can be readily identified and notified based on, *inter alia*, AGH's records and databases.

144. AGH has acted, and has refused to act, on grounds generally applicable to the Class, thereby making appropriate final relief with respect to the Class as a whole.

CAUSES OF ACTION

COUNT I — Negligence
(By Plaintiffs on behalf of the Class, or, in the alternative, the Maryland Subclass)

145. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

146. This count is brought on behalf of all Class members.

147. AGH owed a duty to Plaintiffs and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the Private Information that AGH collected.

148. AGH owed a duty to Plaintiffs and the Class to provide security, consistent with industry standards and requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the Private Information that AGH collected.

149. AGH owed a duty to Plaintiffs and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it was discovered.

150. AGH owed a duty of care to Plaintiffs and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

151. AGH solicited, gathered, and stored the Private Information belonging to Plaintiffs and the Class.

152. AGH knew or should have known it inadequately safeguarded this information.

153. AGH knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiffs and Class members, and AGH was therefore charged with a duty to adequately protect this critically sensitive information.

154. AGH had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' highly sensitive Private Information was entrusted to AGH on the understanding that adequate security precautions would be taken to protect the PII and medical information. Moreover, only AGH had the ability to protect its systems and the Private Information stored on them from attack.

155. AGH's own conduct also created a foreseeable risk of harm to Plaintiffs, Class members, and their PII. AGH's misconduct included failing to: (1) secure its systems, servers and networks, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the safeguards, policies, and procedures necessary to prevent this type of data breach.

156. AGH breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the Private Information belonging to Plaintiffs and the Class.

157. AGH breached its duties to Plaintiffs and the Class by creating a foreseeable risk of harm through the misconduct previously described.

158. AGH breached the duties it owed to Plaintiffs and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of Private Information.

159. The law further imposes an affirmative duty on AGH to timely disclose the unauthorized access and theft of the Private Information belonging to Plaintiffs and the Class so that Plaintiffs and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

160. AGH breached the duties it owed to Plaintiffs and the Class by failing to timely and accurately disclose to Plaintiffs and Class members that their Private Information had been improperly acquired or accessed.

161. Further evidence of AGH's negligence is clear from its violation of statutes and regulations designed to protect consumers and patients from the harm caused by the failure to secure Private Information.

162. HIPAA obligates Covered Entities and Business Associates to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" and "must reasonably safeguard protected health information." 45 CFR § 164.530(c).

163. In the event of a data breach, HIPAA obligates Covered Entities and Business Associates to notify affected individuals, prominent media outlets, and the Secretary of the Department of Health and Human Services of the data breach without unreasonable delay and in no event later than 60 days after discovery of the data breach. 45 CFR § 164.400, *et seq.*

164. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as AGH, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of AGH's duty.

165. The Maryland Consumer Protection Act ("MCPA"), Md. Code Comm. Law § 13-101, *et seq.*, prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the provision of any service. The Maryland Personal Information Protection Act ("PIPA"), Md. Code Comm. Law § 14-3501, *et seq.*, requires businesses collecting and storing consumers' "personal information" to take adequate measures to safeguard this information, and

mandates that in the event of a breach, notice must be given to consumers within 45 days after a breach.

166. AGH violated HIPAA, MCPA, PIPA, and FTC rules and regulations obligating companies to use reasonable measures to protect Private Information by failing to comply with applicable industry standards; and by unduly delaying reasonable notice of the actual breach. AGH's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, the foreseeable consequences of a Data Breach and the exposure of Plaintiffs' and Class members' sensitive Private Information.

167. Plaintiffs and the Class are within the category of persons HIPAA, MCPA, PIPA, and the FTC Act were intended to protect.

168. The harm that occurred as a result of the Data Breach described herein is the type of harm HIPAA, MCPA, PIPA, and FTC Act were intended to guard against.

169. As a direct and proximate result of AGH's conduct, Plaintiffs and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

170. As a direct and proximate result of AGH's negligent conduct, Plaintiffs and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their Private Information in AGH's possession, and are entitled to damages in an amount to be proven at trial.

COUNT II — Breach of Implied Contract
(By Plaintiffs on behalf of the Class, or, in the alternative, the Maryland Subclass)

171. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

172. This count is brought on behalf of all Class members.

173. Plaintiffs and the Class provided AGH with their PII and medical information.

174. By providing their Private Information, and upon AGH's acceptance of such information, Plaintiffs and the Class, on one hand, and AGH, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

175. The implied contracts between AGH and Plaintiffs and Class members obligated AGH to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiffs' and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. AGH expressly adopted and assented to these terms in its public statements, representations and promises as described above.

176. The implied contracts for data security also obligated AGH to provide Plaintiffs and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

177. AGH breached the implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiffs and Class members; allowing unauthorized persons to access Plaintiffs' and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiffs and Class members, as alleged above.

178. As a direct and proximate result of AGH's breaches of the implied contracts, Plaintiffs and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of their PII and medical information in AGH's possession, and are entitled to damages in an amount to be proven at trial.

COUNT III — Bailment
(By Plaintiffs on behalf of the Class, or, in the alternative, the Maryland Subclass)

179. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

180. This count is brought on behalf of all Class members.

181. Plaintiffs' and Class members' Private Information was provided to AGH.

182. In delivering their Private Information, Plaintiffs and Class members intended and understood that their Private Information would be adequately safeguarded and protected.

183. AGH accepted Plaintiffs' and Class members' Private Information.

184. By accepting possession of Plaintiffs' and Class members' Private Information, AGH understood that Plaintiffs and the Class expected their Private Information to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

185. During the bailment (or deposit), AGH owed a duty to Plaintiffs and the Class to exercise reasonable care, diligence, and prudence in protecting their Private Information.

186. AGH breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class members' Private Information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class members' Private Information.

187. AGH further breached its duty to safeguard Plaintiffs' and Class members' Private Information by failing to timely notify them that their Private Information had been compromised as a result of the Data Breach.

188. AGH failed to return, purge, or delete the Private Information belonging to Plaintiffs and Class members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

189. As a direct and proximate result of AGH's breach of its duties, Plaintiffs and the Class suffered consequential damages that were reasonably foreseeable to AGH, including but not limited to the damages set forth herein.

190. As a direct and proximate result of AGH's breach of its duty, Plaintiffs' and Class members' PII that was entrusted to AGH during the bailment (or deposit) was damaged and its value diminished.

COUNT IV — Unjust Enrichment
(By Plaintiffs on behalf of the Class, or, in the alternative, the Maryland Subclass)

191. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

192. This count is brought on behalf of all Class members.

193. Plaintiffs and the Class have an interest, both equitable and legal, in their Private Information that was collected and maintained by AGH.

194. AGH was benefitted by the conferral upon it of Plaintiffs' and Class members' Private Information and by its ability to retain and use that information. AGH understood that it was in fact so benefitted.

195. AGH also understood and appreciated that Plaintiffs' and Class members' Private Information was private and confidential and its value depended upon AGH maintaining the privacy and confidentiality of that information.

196. But for AGH's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class members would not have provided or authorized their Private Information to be provided to AGH, and AGH would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining patients, gaining the reputational advantages conferred upon it by Plaintiffs

and Class members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

197. As a result of AGH's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiffs, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiffs and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information AGH has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class.

198. AGH's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

199. Under the common law doctrine of unjust enrichment, it is inequitable for AGH to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and the Class in an unfair and unconscionable manner. AGH's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

200. The benefit conferred upon, received, and enjoyed by AGH was not conferred officiously or gratuitously, and it would be inequitable and unjust for AGH to retain the benefit.

201. AGH is therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on AGH as a result of its wrongful conduct, including specifically the value

to AGH of the PII and medical information that was accessed and exfiltrated in the Data Breach and the profits AGH receives from the use and sale of that information.

COUNT V — Violation of the Maryland Consumer Protection Act
Md. Code Ann. Comm. Law § 13-101 – 13-501, *et seq.*
(By Plaintiffs on behalf of the Class, or, in the alternative, the Maryland Subclass)

202. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

203. The MCPA prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the provision of commerce. *See* Md. Code Comm. Law § 13-102.

204. AGH's deceptive acts or practices in the conduct of business include, but are not limited to:

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

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

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

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to

the security and privacy of Plaintiffs' and Class members' Private Information; and

h. Failing to promptly and adequately notify Plaintiffs and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

205. AGH's violation of the Maryland Personal Information Protection Act, Md. Code Comm. Law § 14-3501, *et seq.*, also constitutes a per se deceptive business practice under the MCPA. Md. Code Comm. Law § 14-3508.

206. AGH is engaged in, and its acts and omissions affect, trade and commerce. AGH's relevant acts, practices and omissions complained of in this action were done in the course of AGH's business of marketing, offering for sale, and selling goods and services throughout Maryland and the United States.

207. AGH had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiffs' and Class members' Private Information. This exclusive knowledge includes, but is not limited to, information that AGH received through internal and other non-public audits and reviews that concluded that AGH's security policies were substandard and deficient, and that Plaintiffs' and Class members' Private Information and other AGH data was vulnerable.

208. AGH had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

209. AGH also had exclusive knowledge about the length of time that it maintained individuals' Private Information after they stopped using services that necessitated the transfer of that Private Information to AGH.

210. AGH failed to disclose, and actively concealed, the material information it had regarding AGH's deficient security policies and practices, and regarding the security of the

sensitive Private Information. For example, even though AGH has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiffs' and Class members' Private Information was vulnerable as a result, AGH failed to disclose this information to, and actively concealed this information from, Plaintiffs, Class members and the public. AGH also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former patients' Private Information and other records. Likewise, during the days and weeks following the Data Breach, AGH failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

211. AGH had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, and because AGH was in a fiduciary position by virtue of the fact that AGH collected and maintained Plaintiffs' and Class members' Private Information.

212. AGH's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of AGH's data security and its ability to protect the confidentiality of current and former patients' Private Information.

213. Had AGH disclosed to Plaintiffs and the Class that its data systems were not secure and, thus, vulnerable to attack, AGH would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, AGH received, maintained, and compiled Plaintiffs' and Class members' Private Information without advising that AGH's data security practices were insufficient to maintain the safety and confidentiality of their Private Information.

214. Accordingly, Plaintiffs and Class members acted reasonably in relying on AGH's misrepresentations and omissions, the truth of which they could not have discovered.

215. AGH's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as HIPAA and the FTC Act.

216. The injuries suffered by Plaintiffs and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiffs and the Class should have reasonably avoided.

217. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and the Class as a direct result of AGH's deceptive acts and practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their Private Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. damages to and diminution in value of their personal information entrusted to AGH, and with the understanding that AGH would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their Private Information, which remains in the possession of AGH and which is subject to further breaches so long as AGH fails to undertake appropriate and adequate measures to protect data in its possession.

218. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring AGH from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VI — Declaratory Judgment
(By Plaintiffs on behalf of the Class, or, in the alternative, the Maryland Subclass)

219. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

220. This count is brought on behalf of all Class members.

221. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described herein.

222. An actual controversy has arisen in the wake of the Data Breach regarding AGH's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' Private Information, and whether AGH is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information. Plaintiffs alleges that AGH's data security measures remain inadequate.

223. Plaintiffs and the Class continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

224. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that AGH continues to owe a legal duty to secure Plaintiffs' and Class

members' Private Information, to timely notify them of any data breach, and to establish and implement data security measures that are adequate to secure Private Information.

225. The Court also should issue corresponding prospective injunctive relief requiring AGH to employ adequate security protocols consistent with law and industry standards to protect Plaintiffs' and Class members' Private Information.

226. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy. The threat of another breach of the Private Information in AGH's possession, custody, and control is real, immediate, and substantial. If another breach of AGH's network, systems, servers, or workstations occurs, Plaintiffs and the Class will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

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

228. Issuance of the requested injunction will serve the public interest by preventing another data breach at AGH, thus eliminating additional injuries to Plaintiffs and the thousands of Class members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in their favor and against AGH, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

B. That Plaintiffs be granted the declaratory relief sought herein;

C. That the Court grant permanent injunctive relief to prohibit AGH from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiffs and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiffs and the Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

F. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the putative Class, demand a trial by jury on all issues so triable.

Date: March 25, 2024

Respectfully Submitted,

/s/ James P. Ulwick

James P. Ulwick, Federal Bar No. 00536
Jean E. Lewis, Federal Bar No. 27562
KRAMON & GRAHAM, P.A.
One South Street, Suite 2600
Baltimore, Maryland 21202
(410) 752-6030 (tel.)
(410) 539-1269 (fac.)
julwick@kg-law.com
jlewis@kg-law.com

Daniel O. Herrera
Nickolas Hagman
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle St.
Suite 3200
Chicago, IL 60603
Phone: (312) 782-4880
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Thomas Pacheco
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
900 W Morgan Street
Raleigh, NC 27603
T: (212) 946-9305
tpacheco@milberg.com

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

Attorneys for Plaintiffs and the Proposed Class