IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

Michael Rentschler, individually, and on behalf of all others similarly situated, Plaintiff, v. Atlantic General Hospital Corporation Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Michael Rentschler ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this action against Atlantic General Hospital Corporation, ("AGH" or "Defendant"), by and through his attorneys, and alleges, based upon personal knowledge as to his 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, driver's license numbers, information regarding medical treatment, diagnosis, and prescriptions, medical record numbers, health insurance information, other protected health information ("personally identifying information" or "PII"), as well as financial account/payment card information ("financial account 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 privately identifiable information ("PII"), private health information ("PHI"), and financial account information (collectively, "Private Information").

4. According to the data breach notice that AGH sent to affected individuals, on January 29, 2023, AGH discovered suspicious activity in its company networks 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 accessed numerous files. AGH and its contracted specialists then began an investigation into to the Data Breach. On March 6, 2023, AGH determined that unauthorized actor(s) accessed files that contained sensitive information that could identify current and former AGH patients. The sensitive information exposed by then breach included such as 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.

5. Despite determining that unauthorized actors accessed Private Information concerning current and former AGH patients, AGH waited eighteen days before sending out data breach notices to affected individuals, on or about March 24, 2023. AGH's data breach notice is attached as **Exhibit A**.

6. AGH's failure to promptly notify Plaintiff 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 Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

7. 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. Due to AGH's failures, Plaintiff and approximately 30,703 other individuals suffered substantial harm and injury.[1]

8. As a result of AGH's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff's and Class members' Private Information was accessed and acquired by unauthorized third-parties for the express purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of AGH's patients. Plaintiff 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.

9. Plaintiff 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

[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/ (last accessed April 11, 2023).

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 Plaintiff and the Class.

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

II. PARTIES

Plaintiff Michael Rentschler

11. Plaintiff Michael Rentschler is a resident and citizen of Maryland. Plaintiff is a patient of AGH. Plaintiff received AGH's Data Breach Notice.

Defendant Atlantic General Hospital Corporation

12. 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. Atlantic General Hospital employs more than 940 people and generates approximately $138 million in annual revenue.[2]

III. JURISDICTION AND VENUE

13. 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.

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

15. 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 Plaintiff's and Class members' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Atlantic General Hospital – Background

16. 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

[2] *Id*.

and treatment information, health insurance information, driver's license numbers, passport information, financial account information and contact information.

17. 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 30,704 current and former patients.

18. Current and former patients of AGH, such as Plaintiff 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.

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

B. The Data Breach

20. 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.[3]

21. This investigation revealed that intruders had breached AGH's systems starting as early as 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

[3] Ex. A.

stolen information belonged, which took until March 6, 2023–more than one month after AGH discovered suspicious activity on its servers.[4]

22. 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.

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

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

24. 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.[5]

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 Plaintiff's 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

[4] *Id.*

[5] *Id.*

relating to data privacy and security,"[6] implicitly admitting that its information systems policies and protocols were inadequate prior to the Data Breach.

25. AGH's failure to properly safeguard Plaintiff's and Class members' Private Information allowed the unauthorized actors to access this highly valuable information, but AGH's failure to timely notify Plaintiff 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.

26. 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.

27. Second, AGH failed to timely notify affected individuals, including Plaintiff and Class members, that their highly-sensitive Private Information had been accessed by unauthorized third parties. AGH waited approximately two months from the time of discovery to notify victims of the Data Breach that their Private Information had been compromised.

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

[6] *Id.*

29. In short, AGH's myriad failures, including the failure to timely detect the Data Breach and/or notify Plaintiff 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 Plaintiff's and Class members' Private Information for weeks 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

30. 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.

31. 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.[7] 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.[8]

32. 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

[7] *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+ (last accessed March 23, 2023).

[8] *2022 Healthcare Data Breach Report*, The HIPAA Journal (January 24, 2023), available at: https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last accessed March 23, 2023).

157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[9] 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%. [10]

33. Data breaches are a constant threat because PII is routinely traded on the dark web as s 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.[11]

34. 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.[12]

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

---

[9] *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/ (last accessed last accessed March 23, 2023).

[10] *Id.*

[11] *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/ (last accessed March 23, 2023).

[12] 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 (last accessed March 23, 2023).

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.[13]

35. 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.[14] 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".[15] With this bounty of ill-gotten information, cybercriminals can wreak havoc and perpetuate far serious crimes such as drug dealing (by obtaining prescriptions under the victims' names) and major fraud (by filing large-scale and bogus insurance claims).[16]

36. 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

---

[13] *Id.*

[14] 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 (last accessed March 23, 2023).

[15] *Id.*

[16] *Id.*

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).[17] 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 stockpile prescription drugs for sale in the drug trade.[18]

37. 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.[19]

38. 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.[20]

39. 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

---

[17] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html (last accessed March 23, 2023).

[18] *Id.*

[19] *Id.*

[20] 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 (last accessed March 11, 2023).

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.[21]

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

41. 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.

42. 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 Plaintiff's and Class members' Private Information can easily obtain Plaintiff's and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

43. 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

[21] *See e.g.*, *Healthcare Data Breach Statistics*, HIPAA Journal, available at: https://www.hipaajournal.com/healthcare-data-breach-statistics (last accessed March 11, 2023).

breach, because credit card victims can cancel or close credit and debit card accounts.[22] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

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

45. 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 Plaintiff and the Class from misappropriation. As a result, the injuries to Plaintiff 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

46. AGH has an obligation, both statutory and self-imposed, to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's 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. Plaintiff and Class

[22] *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 (last accessed March 11, 2023).

members provided, and AGH obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

47. 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.*

48. 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.*

49. 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.

50. Additionally, 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.*

51. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[23] 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."[24]

52. 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.[25]

53. 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.[26] 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.[27] 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

[23] 17 C.F.R. § 248.201 (2013).

[24] *Id.*

[25] *Start With Security*, Federal Trade Commission (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[26] *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.

[27] *Id.*

of data being transmitted from the system; and have a response plan ready in the event of a breach.[28] 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.

54. Here, at all relevant times, AGH was fully aware of its obligation to protect the PII Private Information of its current and former patients, including Plaintiff 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 patients' PII, protected health information, and medical information in order to operate its business.

55. 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 Plaintiff and Class members. AGH alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' Private Information.

56. 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.

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

[28] *Id.*

F. AGH Violated HIPAA, FTC and Industry Standard Data Protection Protocols

58. 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.

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

60. 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.

61. 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 Plaintiff and Class members.

62. 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 failed in, *inter alia*, the following respects:

a. Developing and employing adequate intrusion detection systems;

b. Engaging in regular reviews of audit logs and authentication records;

c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;

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

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

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

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

h. Implementing 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.

63. 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 its Self-Imposed Data Security Obligations

64. 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.[29]

65. Plaintiff's and Class members' provided their Private Information to AGH in reliance on its promises and self-imposed obligations to keep PII and medical information

[29] *Atlantic Genera Hospital Privacy Policy*, Atlantic General Hospital, available at https://www.atlanticgeneral.org/patients-visitors/privacy-policy/ (last accessed April 12, 2023).

confidential, and to secure the Private Information from unauthorized access by malevolent actors. It failed to do so.

66. 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.

67. Indeed, following the Data Breach, AGH effectively conceded that its security practices were inadequate and ineffective. In the Notice it sent to Plaintiff and others, AGH acknowledged that the Data Breach required it to add "additional safeguards."[30]

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

68. Like any data hack, the Data Breach presents major problems for all affected.[31]

69. 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, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[32]

70. The ramifications of AGH's failure to properly secure Plaintiff's and Class members' Private Information are severe. Identity theft occurs when someone uses another

[30] Ex. A.

[31] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers (last accessed March 23, 2023).

[32] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed March 11, 2023).

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.

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

72. 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.

73. Accordingly, AGH's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[33] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[34] 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."[35] 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.

---

[33] *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 (last accessed March 11, 2023).

[34] 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 (last accessed March 11, 2023).

[35] 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) (last accessed March 11, 2023).

74. 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 outstrips the increase in incidence of traditional identity theft.[36] 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.[37]

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

76. 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.

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

a. Theft of Private Information;

[36] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html (last accessed March 23, 2023).

[37] *Id.*

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 Plaintiff's and Class members' privacy.

78. Plaintiff 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 Plaintiff's and Class members' Private Information, especially their Social Security numbers, puts Plaintiff 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 to two years of credit monitoring that AGH offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiff and Class members have suffered and will continue to suffer as a result of the Data Breach.

79. As a direct and proximate result of AGH's acts and omissions in failing to protect and secure Private Information, Plaintiff 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.

80. Plaintiff retains 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 himself and similarly situated individuals whose Private Information was accessed in the Data Breach.

I. Plaintiff Michael Rentschler's Experience

81. 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.

82. 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.

83. 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.

84. 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.

85. 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.

V. CLASS ALLEGATIONS

86. Plaintiff brings this action on behalf of himself/herself 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.

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

87. In the alternative, Plaintiff brings this action on behalf of himself 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 (the "Maryland Subclass").

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

88. 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 30,704.[38] 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 Plaintiff only through the discovery process. The members of the Class will be identifiable through information and records in AGH's possession, custody, and control.

89. 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 Plaintiff 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 Plaintiff's and Class members' Private Information;

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

[38] 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/ (last accessed April 11, 2023).

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

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

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

91. Adequacy: Plaintiff is an adequate representative because his 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. Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor his counsel have any interests that are antagonistic to the interests of other members of the Class.

92. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff 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.

93. AGH has acted, and 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 Plaintiff on behalf of the Class, or, in the alternative, the Maryland Subclass)

94. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

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

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

97. AGH owed a duty to Plaintiff 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.

98. AGH owed a duty to Plaintiff 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 is discovered.

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

100. AGH solicited, gathered, and stored the Private Information belonging to Plaintiff and the Class.

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

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

103. AGH had a special relationship with Plaintiff and Class members. Plaintiff's 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.

104. AGH's own conduct also created a foreseeable risk of harm to Plaintiff, 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.

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

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

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

108. The law further imposes an affirmative duty on AGH to timely disclose the unauthorized access and theft of the Private Information belonging to Plaintiff and the Class so

that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

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

110. AGH breached its duty to timely notify Plaintiff and Class members of the Data Breach by failing to provide direct notice to Plaintiff and the Class concerning the Data Breach until on or about March 24, 2023.

111. As a direct and proximate result of AGH's conduct, Plaintiff 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.

112. As a direct and proximate result of AGH's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II — Negligence *Per Se*
(By Plaintiff on behalf of the Class, or, in the alternative, the Maryland Subclass)

113. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

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

115. 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).

116. 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.*

117. 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.

118. 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.

119. 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.

120. In addition to the FTC rules and regulations, MCPA, and PIPA, other states and jurisdictions where victims of the Data Breach are located require that AGH protect Private Information from unauthorized access and disclosure, and timely notify the victim of a data breach.

121. 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 Plaintiff's and Class members' sensitive Private Information.

122. AGH's violations of HIPAA, MCPA, PIPA, Section 5 of the FTC Act and other applicable statutes, rules, and regulations constitutes negligence *per se*.

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

124. 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.

125. As a direct and proximate result of AGH's negligence *per se*, Plaintiff 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 III — Breach of Implied Contract
(By Plaintiff on behalf of the Class, or, in the alternative, the Maryland Subclass)

126. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

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

128. Plaintiff and the Class provided AGH with their PII and medical information.

129. By providing their Private Information, and upon AGH's acceptance of such information, Plaintiff 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.

130. The implied contracts between AGH and Plaintiff and Class members obligated AGH to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's 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.

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

132. 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 Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

133. As a direct and proximate result of AGH's breaches of the implied contracts, Plaintiff 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 IV — Bailment
(By Plaintiff on behalf of the Class, or, in the alternative, the Maryland Subclass)

134. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

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

136. Plaintiff's and Class members' Private Information was provided to AGH.

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

138. AGH accepted Plaintiff's and Class members' Private Information.

139. By accepting possession of Plaintiff's and Class members' Private Information, AGH understood that Plaintiff 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.

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

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

142. AGH further breached its duty to safeguard Plaintiff's 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.

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

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

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

COUNT V — Intrusion Upon Seclusion
(By Plaintiff on behalf of the Class, or, in the alternative, the Maryland Subclass)

146. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

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

148. Plaintiff and Class members had a reasonable expectation of privacy in the Private Information that AGH possessed and/or continues to possess.

149. By failing to keep Plaintiff's and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, AGH invaded Plaintiff's and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiff and Class members, which is highly offensive to a reasonable person.

150. AGH knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider AGH's actions highly offensive.

151. AGH invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

152. As a proximate result of such misuse and disclosures, Plaintiff's and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. AGH's conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

153. In failing to protect Plaintiff's and Class members' Private Information, and in misusing and/or disclosing their Private Information, AGH has acted with malice and oppression and in conscious disregard of Plaintiff's and the Class members rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its millions of patients. Plaintiff, therefore, seek an award of damages, including punitive damages, on behalf of Plaintiff and the Class.

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

154. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

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

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

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

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

159. But for AGH's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provide 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 Plaintiff 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.

160. As a result of AGH's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiff, 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 Plaintiff 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, Plaintiff and the Class.

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

162. 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 Plaintiff 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.

163. 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.

164. AGH is therefore liable to Plaintiff 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 VII — Violation of the Maryland Consumer Protection Act
Md. Code Ann. Comm. Law § 13-101 – 13-501, *et seq.*
(By Plaintiff on behalf of the Class, or, in the alternative, the Maryland Subclass)

165. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

166. 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.

167. 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 Plaintiff's 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 Plaintiff's 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 Plaintiff's 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 Plaintiff's and Class members' Private Information;

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

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

168. 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.

169. AGH had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiff's 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 Plaintiff's and Class members' Private Information and other AGH data was vulnerable.

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

171. 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.

172. 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 Plaintiff's and Class members' Private Information was vulnerable as a result, AGH failed to disclose this information to, and actively concealed this information from, Plaintiff, 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.

173. 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 Plaintiff's and Class members' Private Information.

174. 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.

175. Had AGH disclosed to Plaintiff 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 Plaintiff's 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.

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

177. 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.

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

179. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff 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.

180. Plaintiff 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 VIII — Violation of State Data Breach Statutes
(By Plaintiff on behalf of the Class)

181. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

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

183. AGH is a corporation that owns, maintains, and records Private Information, and computerized data including Private Information, about its current and former patients, including Plaintiff and Class members.

184. AGH is in possession of Private Information belonging to Plaintiff and Class members and is responsible for reasonably safeguarding that Private Information consistent with the requirements of the applicable laws pertaining hereto.

185. AGH failed to safeguard, maintain, and dispose of, as required, the Private Information within its possession, custody, or control as discussed herein, which it was required to do by all applicable State laws.

186. AGH, knowing and/or reasonably believing that Plaintiff's and Class members' Private Information was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members as required by following data breach statutes.

187. AGH's failure to provide timely and accurate notice of the Data Breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;

b. Ark. Code Ann. § 4-110-105(a), *et seq.*;

c. Cal. Civ. Code § 1798.80, *et seq.*;

d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;

e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;

f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;

g. D.C. Code § 28-3852(a), *et seq.*;

h. Fla. Stat. Ann. § 501.171(4), *et seq.*;

i. Ga. Code Ann. § 10-1-912(a), *et seq.*;

j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;

k. Idaho Code Ann. § 28-51-105(1), *et seq.*;

l. Illinois Statute 815 ILCS 530/1, *et seq.*;

m. Iowa Code Ann. § 715C.2(1), *et seq.*;

n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;

s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;

u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;

v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;

w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;

bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;

cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

dd. R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), *et seq.*;

ee. S.C. Code Ann. § 39-1-90(A), *et seq.*;

ff. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

gg. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq.*;

hh. Utah Code Ann. § 13-44-202(1), *et seq.*;

ii. Va. Code. Ann. § 18.2-186.6(B), *et seq.*;

jj. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;

kk. Wis. Stat. Ann. § 134.98(2), *et seq.*; and

ll. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

188. As a result of AGH's failure to reasonably safeguard Plaintiff's and Class members' Private Information, and the failure to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members, Plaintiff 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 IX — Violation of State Consumer Protection Statutes
(By Plaintiff behalf of the Class)

189. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

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

191. AGH is a "person" as defined in the relevant state consumer statutes.

192. AGH engaged in the conduct alleged herein that was intended to result, and which did result, in the trade and commerce with Plaintiff and Class members. AGH is engaged in, and its acts and omissions affect, trade and commerce. Further, AGH's conduct implicates consumer protection concerns generally.

193. AGH's acts, practices and omissions were done in the course of AGH's business of marketing, facilitating, offering for sale, and selling goods and services throughout the United States.

194. AGH's unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's 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 was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information, including but not limited to duties imposed by the FTC Act and similar state laws, rules, and regulations, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's 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 Plaintiff's and the Class members' Private Information;

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

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

195. By engaging in such conduct and omissions of material facts, AGH has violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods and services are of a particular standard, quality or grade, if they are of another", and/or "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding"; and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

196. AGH's representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of AGH's data security and ability to protect the confidentiality of Private Information.

197. AGH intentionally, knowingly, and maliciously misled Plaintiff and Class members and induced them to rely on its misrepresentations and omissions.

198. Had AGH disclosed that its data systems were not secure and, thus, vulnerable to attack, it would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, AGH received, maintained, and compiled Plaintiff's 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. Accordingly, Plaintiff and the Class members acted reasonably in relying on AGH's misrepresentations and omissions, the truth of which they could not have discovered.

199. Past breaches within the industry put AGH on notice that its security and privacy protections were inadequate.

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

201. The harm these practices caused to Plaintiff and the Class members outweighed their utility, if any.

202. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and Class members as a direct result of AGH's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or 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 and medical 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.

203. AGH's conduct described herein, including without limitation, AGH's failure to maintain adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information, AGH's failure to disclose the material fact that it did not have adequate computer systems and safeguards to adequately protect Plaintiff's and Class members' Private Information, AGH's failure to provide timely and accurate notice to of the material fact of the Data Breach, and AGH's continued acceptance of Plaintiff's and Class members' Private Information constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of the following state consumer statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5(5), (7) and (27), *et seq.*;

b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

c. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), *et seq.*;

d. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*, and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq.*;

e. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq.*;

f. The Delaware Deceptive Trade Practices Act, Del. Code Ann. Title 6, § 2532(5) and (7), *et seq.*, and the Delaware Consumer Fraud Act, Del. Code Ann. Title 6 § 2513, *et seq.*;

g. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq.*;

h. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (5) and (7), *et seq.*;

i. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), *et seq.*; and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq.*;

j. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq.*; and Idaho Code § 48-603C, *et seq.*;

k. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*;

l. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), *et seq.*;

m. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, *et seq.*;

n. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), *et seq.*;

o. The Kentucky Consumer Protection Act, K.R.S. § 367.170(1) and (2), *et seq.*;

p. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq.*;

q. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), e*t seq.*, and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, *et seq.*;

r. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), *et seq.*;

s. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), *et seq.*;

t. The Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c)(e),(s) and (cc), *et seq.*;

u. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), et seq., the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);

v. The Mississippi Consumer Protection Act, Miss. Code Ann. §§ 75-24-5(1), (2)(e) and (g), *et seq.*;

w. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq.*;

x. The Montana Unfair Trade Practices and Consumer Protection Act, MCA §§ 30-14-103, *et seq.*;

y. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq.*;

z. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7), *et seq.*;

aa. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), *et seq.*;

bb. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;

cc. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, *et seq.*;

dd. New York Business Law, N.Y. Gen. Bus. Law § 349(a);

ee. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq.*;

ff. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, *et seq.*;

gg. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and (B)(1) and (2), *et seq.*;

hh. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. § 753(5), (7) and (20), *et seq.*; and the Oklahoma Deceptive Trade Practices Act, 78 Okl. Stat. Ann. § 53(A)(5) and (7), *et seq.*;

ii. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e)(g) and (u), *et seq.*;

jj. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq.*;

kk. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), *et seq.*;

ll. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq.*;

mm. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), *et seq.*;

nn. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a) and (b)(5) and (7);

oo. The Texas Deceptive Trade Practices- Consumer Protection Act, V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq.*;

pp. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1) and (2)(a) and (b);

qq. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), *et seq.*;

rr. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5)(6) and (14), *et seq.*;

ss. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq.*;

tt. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq.*;

uu. The Wisconsin Deceptive Trade Practices Act, W.S.A. § 100.20(1), *et seq.*; and

vv. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i), (iii) and (xv), *et seq*.

204. Plaintiff and Class members 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 X — Declaratory Judgment
(By Plaintiff on behalf of the Class, or, in the alternative, the Maryland Subclass)

205. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

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

207. 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.

208. 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 Plaintiff's and Class members' Private Information, and whether AGH is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Private Information. Plaintiff alleges that AGH's data security measures remain inadequate.

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

210. 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 Plaintiff's 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.

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

212. If an injunction is not issued, Plaintiff 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, Plaintiff 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.

213. The hardship to Plaintiff 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, Plaintiff 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.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in his 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 Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

B. That Plaintiff 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 Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

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

F. That the Court award to Plaintiff 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

Plaintiff, on behalf of himself and the putative Class, demands a trial by jury on all issues so triable.

Date: April 13, 2023

Respectfully submitted,

/s/ James P. Ulwick

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

Daniel O. Herrera
Nickolas J. Hagman
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org
