UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

ROBERT SCHULTE JR., individually and on behalf of all others similarly situated, Plaintiff, v. NUANCE COMMUNICATIONS, INC. and GEISINGER HEALTH d/b/a GEISINGER HEALTH FOUNDATION, Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Robert Schulte Jr. ("Plaintiff") individually and on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Nuance Communications, Inc. ("Nuance") and Geisinger Health d/b/a Geisinger Health Foundation ("GH" and collectively with Nuance, "Defendants"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff brings this class action lawsuit against Defendants for failure to properly secure and safeguard Plaintiff and Class Members' personally

identifiable information ("PII")[1] and protected health information ("PHI," and collectively with PII, "Private Information") including dates of birth, addresses, admit, discharge and transfer codes, medical record numbers, race, gender, phone numbers and facility name abbreviations.

2. Nuance is a computer software technology corporation based out of Burlington, Massachusetts.[2] Nuance is an IT vendor of GH, which is a regional health care provider headquartered in Danville, Pennsylvania.[3]

3. On or around November 29, 2023, GH discovered that a former Nuance employee had accessed certain Geisinger patient information two days after the employee had been terminated.[4] Following an investigation, Nuance determined that more than one million GH patients were impacted by the data breach (the "Data Breach").[5] Nuance, on behalf of GH, began sending out notice letters to individuals impacted on June 21, 2024.

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] *Who We Are,* NUANCE, https://www.nuance.com/company-overview/who-we-are.html (last visited July 2, 2024).

[3] *About Geisinger*, GEISINGER, https://www.geisinger.org/about-geisinger/who-we-are (last visited July 2, 2024).

[4] *Geisinger provides notice of Nuance's data security incident*, GEISINGER (June 24, 2024) https://www.geisinger.org/about-geisinger/news-and-media/news-releases/2024/06/24/18/17/geisinger-provides-notice-of-nuances-data-security-incident (last visited July 2, 2024).

[5] *Id.*

4. Defendants had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on their affirmative representations to Plaintiff and the Class, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. Defendants failed to take precautions designed to keep patients' Private Information secure.

6. Defendants owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendants solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

7. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their Private Information and are subject to an increased risk of identity theft.

8. Defendants, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive information maintained, causing the exposure of Private Information for Plaintiff and Class Members.

9. As a result of the Defendants' inadequate digital security, Plaintiff's and Class Members' Private Information was accessed by an unauthorized third party. Plaintiff and Class Members have suffered and will continue to suffer injuries including financial losses caused by misuse of Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and medical information.

10. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendants' failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendants conduct amounts to at least negligence and violates federal and state statutes.

11. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendants for: negligence; negligence per se; breach of implied contract; and unjust enrichment.

12. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal

data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

PARTIES

Plaintiff

13. Plaintiff Robert Schulte Jr. is a citizen of Pennsylvania and resides in Dunmore. Plaintiff Schulte is a patient of Geisinger Health. On June 21, 2024, Nuance sent plaintiff Schulte a notice letter informing him that he was impacted by the Data Breach. As a result of the Data Breach, plaintiff Schulte has experienced an uptick in spam calls, texts, and emails. Furthermore, as a result of the Data Breach, plaintiff Schulte has been forced to, and will continue to, invest significant time monitoring his accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, plaintiff Schulte is now subject to substantial and imminent risk of future harm. Had Plaintiff Schulte known that Defendants do not adequately protect the Personal Information in their Possession, Plaintiff Schulte would not have agreed to provide Defendants with his Personal Information or obtained healthcare services from GH.

Defendants

14. Defendant Nuance Communications, Inc. is a Delaware corporation with its principal place of business located in Burlington, Massachusetts. Nuance is a provider of computer software technology.

15. Defendant Geisinger Health d/b/a Geisinger Health Foundation is a Pennsylvania corporation headquartered in Danville, Pennsylvania. Geisinger is a regional health care provider to central, south-central and northeastern Pennsylvania.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than one Defendant, and there are more than 100 putative Class Members.

17. This Court has personal jurisdiction over GH because GH is registered to do business, and maintains its principal place of business, in Danville, Pennsylvania.

18. This Court has specific personal jurisdiction over Nuance because Nuance purposely availed themselves of Pennsylvania by serving as a vendor that provides information technology services to GH.

19. Venue is proper in these District under 28 U.S.C. § 1391(b)(2) because GH is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendants

20. Defendant Nuance is a provider of information technology services.

21. Defendant GH is a regional health care provider to central, south-central and northeastern Pennsylvania.

22. In the ordinary course of their business practices, Defendants store, maintain, and use individuals' Private Information.

23. Upon information and belief, Defendants made promises and representations to consumers, including Plaintiff and Class Members, that the Private Information collected from them would be kept safe, confidential, and that the privacy of that information would be maintained.

24. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

25. As a result of collecting and storing the Private Information of Plaintiff and Class Members for their own financial benefit, Defendants had a continuous duty to adopt and employ reasonable measures to protect Plaintiff and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

26. On or around November 29, 2023, GH detected unusual activity within its IT network.[6] GH determined that a former employee of Nuance, which provides information technology services for GH, had accessed GH patient information two days after the employee had been terminated.[7] Upon learning this, Nuance permanently disconnected its former employee's access to GH patient records.[8]

27. In response, Defendants launched an investigation with the help of third-party data security experts and law enforcement.[9] The investigation determined that more than one million GH patients' sensitive personal information was compromised in the Data Breach.[10]

28. The investigation determined that the following types of Private Information were compromised in the Data Breach: full names, dates of birth,

---

[6] Sara Scinto, *Information on one million Geisinger patients involved in data breach,* WVIA (June 26, 2024), https://www.wvia.org/news/local/2024-06-26/information-on-one-million-geisinger-patients-involved-in-data-breach (last visited July 2, 2024).
[7] *Id.*
[8] *Geisinger: 1M patients affected by data breach,* THE EXPRESS (June 26, 2024), https://www.lockhaven.com/news/local-news/2024/06/geisinger-1m-patients-affected-by-data-breach/ (last visited July 2, 2024).
[9] *Id.*
[10] *Id.*

addresses, admit, discharge and transfer codes, medical record numbers, race, gender, phone numbers and facility name abbreviations.[11]

29. Nuance, on behalf of GH, began notifying impacted individuals on June 21, 2024.

30. While Defendants sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive personal information of Plaintiff and Class Members.

31. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendants' Failure to Prevent, Identify and Timely Report the Data Breach

32. Defendants admit that an unauthorized third person accessed their IT network in order to obtain sensitive information about their current and former consumers.

33. Defendants are not only aware of the importance of protecting the Private Information that it maintains, as alleged, they each promote their capability to do so.[12]

---

[11] *Id.*

[12] *Nuance Privacy Statement*, NUANCE, https://www.nuance.com/about-us/company-policies/privacy-policies.html (last visited July 2, 2024); *Website Privacy Policy*, Geisinger (updated May 3, 2023) , https://www.geisinger.org/about-

34. The Private Information that Defendants allowed to be exposed in the Data Breach is the type of private information that Defendants knew or should have known would be the target of cyberattacks, and the type of private information Defendants knew are protected under statutory law.

35. Despite their own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[13] Defendants failed to disclose that their systems and security practices were inadequate to reasonably safeguard their consumers sensitive Private Information.

36. Furthermore, despite being aware of the Data Breach on November 29, 2023, Defendants did not begin notifying impacted individuals until June 21, 2024, more than six months later.

D. Data Breaches Cause Disruptions That Put Patients at an Increased Risk of Harm

37. Cyber-attacks at medical facilities, such as the GH facilities, are especially problematic because of the disruption they cause to the health treatment and overall daily lives of patients affected by the attack.

---

geisinger/corporate/corporate-policies/website-privacy-policy (last visited July 2, 2024).

[13] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited July 2, 2024).

38. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment due to a disruption of service. This leads to a deterioration in the quality of overall care patients receive at facilities affected by cyber-attacks and related data breaches.

39. Researchers have found medical facilities that experience a data security incident incur an increase in the death rate among patients' months and years after the attack.[14] Researchers have further found that at medical facilities that experience a data breach, the incident leads to a deterioration in patient outcomes, generally.[15]

E. The Harm Caused by the Data Breach Now and Going Forward

40. Victims of data breaches are susceptible to becoming victims of identity theft.

41. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can

[14] *See* Nsikan Akpan, *Ransomware and data Breaches linked to uptick in fatal heart attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last accessed July 2, 2024).

[15] *See* Sung J. Choi PhD., et al., *Data breach remediation efforts and their implications for hospital quality*, HEALTH SERVICES RESEARCH (Sept. 10, 2019) available at: https://onlinelibrary.wiley.com/doi/abs/10.1111/1475-6773.13203 (last visited July 2, 2024).

drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[16]

42. The type of data that was accessed and compromised here can be used to perpetrate fraud and identity theft. Names, addresses and dates of birth together constitute high risk data.

43. Plaintiff and Class members face a substantial risk of identity theft given that their addresses, dates of birth, and other important Private Information were compromised in the Data Breach. Once these types of Private Information are stolen, they can be used to identify victims and target them in fraudulent schemes and identity theft.

44. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

45. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for

[16] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited July 2, 2024).

profit.[17]

46. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, someone can purchase a full range of documents that will allow identity theft, including $500 for a high-quality U.S. driver's license, $25 for a hacked social media account, $110 for credit card information, and $150 for banking account information.[18] The Private Information compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information are worth more than 10 times on the black market."[19]

47. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to

[17] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (updated Feb. 1, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited July 2, 2024).

[18] Ryan Smith, *Revealed – how much is personal information worth on the dark web?,* INSURANCEBUSINESS (May 1, 2023) https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx (last visited July 2, 2024).

[19] *Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (Last visited July 2, 2024).

individuals and business victims.[20]

48. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[21] Defendants did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen.

49. As a result of the Data Breach, the Private Information of Plaintiff and Class Members have been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered thereby as a direct result of Defendants' Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to

[20] *2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (Last visited July 2, 2024).

[21] *Id.*

Defendants' with the mutual understanding that Defendants' would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further injurious breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

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

51. Defendants disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (b) failing to disclose that they do not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

52. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate and continuing increased risk of harm for

identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendants' wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

53. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the Data Breach publicly announced by Nuance in June of 2024 (the "Class").

54. Specifically excluded from the Class and Subclass are Defendants, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendants, and their heirs, successors, assigns, or other persons or

entities related to or affiliated with Defendants and/or their officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

55. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

56. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

57. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendants, upon information and belief, Plaintiff estimates that the Class is comprised of more than one million Class Members. The Class is sufficiently numerous to warrant certification.

58. Typicality of Claims (Rule 23(a)(3)): Plaintiff's claims are typical of those of other Class Members because, Plaintiff, like the unnamed Class, had his Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendants.

59. Adequacy of Representation (Rule 23(a)(4)): Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

60. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendants will likely continue their wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

61. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendants' storage of Class Member's Private Information was done in a negligent manner;

d. Whether Defendants had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;

e. Whether Defendants' conduct was negligent;

f. Whether Defendants' conduct violated Plaintiff's and Class Members' privacy;

g. Whether Defendants' took sufficient steps to secure Plaintiff's and Class Members' Private Information;

h. Whether Defendants were unjustly enriched; and

i. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

62. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude their maintenance as a class action.

63. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendants. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

64. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

65. Given that Defendants had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

66. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 13 and paragraphs 21 through 53 as though fully set forth herein.

67. Plaintiff brings this claim individually and on behalf of the Class Members.

68. Defendants knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

69. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

70. Defendants had, and continues to have, a duty to timely disclose that

Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

71. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its patients' Private Information.

72. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and GH's patients. Defendants were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

73. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

74. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

75. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff and Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

76. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

77. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

78. Defendants, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

79. Defendants breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45,

Defendants failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' Private Information. In violation of the FTC guidelines, *inter alia,* Defendants did not protect the personal patient information they keep.

80. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

81. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

82. Defendants' breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

83. But for Defendants' negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

84. As a result of Defendants' failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

85. As a result of Defendants' negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

86. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 13 and paragraphs 21 through 53 as though fully set forth herein.

87. Section 5 of the FTC 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 Defendants of failing to use reasonable measures to protect

Plaintiff's and Class members' Private Information. Various FTC publications and orders also form the basis of Defendants duty.

88. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class members' Private Information and not complying with industry standards.

89. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

90. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

91. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

92. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

93. As a result of Defendants' negligence, Plaintiff and the other Class members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated

with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members against GH)

94. Plaintiff incorporates by reference and re-allege each and every allegation set forth above in paragraphs 1 through 13 and paragraphs 21 through 53 as though fully set forth herein.

95. Plaintiff and the Class provided and entrusted their Private Information to GH. Plaintiff and the Class provided their Private Information to GH as part of Defendants' regular business practices.

96. In so doing, Plaintiff and the Class entered into implied contracts with GH by which GH agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by GH. Implied in these exchanges was a promise by GH to ensure that the Private Information of Plaintiff and Class Members in its possession was secure.

97. Pursuant to these implied contracts, Plaintiff and Class Members provided GH with their Private Information in order for GH to provide services, for which GH is compensated. In exchange, Defendants agreed to, among other things, and Plaintiff and the Class understood that GH would: (1) provide services to Plaintiff and Class Members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' Private Information; and (3) protect Plaintiff's and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

98. Implied in these exchanges was a promise by GH to ensure the Private Information of Plaintiff and Class Members in its possession was only used to provide the agreed-upon reasons, and that GH would take adequate measures to protect Plaintiff's and Class Members' Private Information.

99. A material term of this contract is a covenant by GH that it would take reasonable efforts to safeguard that information. GH breached this covenant by allowing Plaintiff's and Class Members' Private Information to be accessed in the Data Breach.

100. Indeed, implicit in the agreement between GH and its patients was the obligation that both parties would maintain information confidentially and securely.

101. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class Members would provide their Private

Information in exchange for services by GH. These agreements were made by Plaintiff and Class Members as GH patients.

102. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to GH but for the prospect of utilizing GH's services. Conversely, GH presumably would not have taken Plaintiff's and Class Members' Private Information if it did not intend to provide Plaintiff and Class Members with its services.

103. GH was therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and/or use.

104. Plaintiff and Class Members accepted GH's offer of services and fully performed their obligations under the implied contract with GH by providing their Private Information, directly or indirectly, to GH, among other obligations.

105. Plaintiff and Class Members would not have entrusted their Private Information to GH in the absence of their implied contracts with GH and would have instead retained the opportunity to control their Private Information.

106. GH breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' Private Information.

107. GH's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

108. Instead of spending adequate financial resources to safeguard Plaintiff's and Class Members' Private Information, which Plaintiff and Class Members were required to provide to GH, GH instead used that money for other purposes, thereby breaching their implied contracts it had with Plaintiff and Class Members.

109. As a proximate and direct result of GH's breaches of their implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and All Class Members)

110. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 13 and paragraphs 21 through 53 as though fully set forth herein.

111. Plaintiff and Class Members conferred a benefit upon Defendants by using Defendants' services.

112. Defendants appreciated or had knowledge of the benefits conferred upon themselves by Plaintiff. Defendants benefited from the receipt of Plaintiff and Class Members' Private Information.

113. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and the Class Members' services and their Private Information because Defendants failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendants or utilized their services, either directly or indirectly, had they known Defendants would not adequately protect their Private Information.

114. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seek judgment against Defendants, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and his counsel as Class Counsel;

(b) For an order declaring the Defendants' conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: July 2, 2024

Respectfully submitted,

LYNCH CARPENTER

By: */s/ Gary F. Lynch*

Gary F. Lynch (PA 56887)
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
Email: gary@lcllp.com

Courtney E. Maccarone*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: cmaccarone@zlk.com

Counsel for Plaintiff

**pro hac vice* forthcoming