Exhibit A

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

In re Geisinger Health Data Security Incident Litigation	Case No. 4:24-CV-01071-MWB **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Amber Lopez, Thomas Wilson, Brenda Everett, Ralph Reviello, and James Wierbowski (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated individuals (the "Class" or "Class Members"), file this Consolidated Class Action Complaint ("Complaint") against Defendants Geisinger Health ("Geisinger") and Nuance Communications, Inc. ("Nuance" and, with Geisinger, "Defendants"), and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Healthcare providers and vendors in the healthcare industry that are entrusted with patients' sensitive personally identifying information ("PII") or protected health information ("PHI")[1] owe a duty of care to those individuals to

[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.

protect that information. This duty arises because it is foreseeable that the exposure of PII and PHI to unauthorized persons—especially hackers and other cybercriminals with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health information. It is also foreseeable that entities entrusted with this type of sensitive data are targets for such an attack.

2. Plaintiffs bring this class action against Defendants for their failure to secure and safeguard Plaintiffs' and Class Members' PII and PHI, including their names, birthdates, addresses, admit, discharge or transfer codes, medical record numbers, race, gender, phone numbers, and care location information.

3. Geisinger is a healthcare provider serving urban and rural communities in Pennsylvania, while Nuance is a computer software technology corporation based in Massachusetts.[2] Geisinger selected Nuance to perform information technology work on its behalf. In connection with this work, Geisinger provided Nuance with the sensitive PII and PHI of its patients.

4. On or about November 29, 2023, Geisinger discovered that a former Nuance employee named Andre J. Burk (a/k/a Max Vance) had accessed and acquired the Private Information of Plaintiffs and Class Members that had been

[2] *See Who We Are*, NUANCE, https://www.nuance.com/company-overview/who-we-are.html (last accessed Mar. 13, 2025).

provided by Geisinger to Nuance. This will be referred to hereinafter as the "Data Breach."

5. Mr. Vance reportedly accessed this sensitive data two days *after* he was terminated by Nuance. As noted above, it was Geisinger – not Nuance – that discovered the breach. It was only after this revelation that "Nuance permanently disconnected its former employee's access to Geisinger's records."[3]

6. Following an investigation, Nuance determined that more than one million Geisinger patients were impacted by the Data Breach. Nuance, on behalf of Geisinger, began sending notice letters to individuals impacted on or around June 24, 2024.[4]

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

8. Defendants promised Plaintiffs and Class Members that they, or the third parties they contract and share Private Information with, would implement and

[3] *See 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 (the "Data Breach Notice").
[4] *Id.*

maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiffs' and Class Members' Private Information against unauthorized access and disclosure. Defendants breached those promises by, *inter alia*, failing to adequately protect Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure.

9. Defendants owed Plaintiffs and Class Members a duty to take all reasonable and necessary measures to keep the Private Information they collected safe and secure from unauthorized access. Geisinger, as the entity collecting the PII and PHI, had a non-delegable duty to act reasonably to safeguard this data, and to ensure that any third-party with which it shared this sensitive information would have adequate security measures in place.

10. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiffs and Class Members have been harmed. Plaintiffs and Class Members have lost the ability to control their Private Information and are subject to an increased risk of identity theft. Indeed, several Plaintiffs have already experienced fraud and identity theft subsequent to the Data Breach.

11. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiffs' and Class Members' Private Information was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves

and all persons whose Private Information was exposed as a result of the Data Breach.

12. Plaintiffs, on behalf of themselves and all other Class Members, assert claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, breach of third-party beneficiary contract, and unjust enrichment, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiffs

Plaintiff Amber Lopez

13. Plaintiff Lopez is a citizen and resident of the Commonwealth of Pennsylvania.

14. Plaintiff Lopez obtained healthcare services from Geisinger. As a condition of providing healthcare services to Plaintiff Lopez, Geisinger required Plaintiff Lopez to provide it with her Private Information. Geisinger in turn shared Plaintiff Lopez's Private Information with Nuance.

15. Plaintiff Lopez believed that Defendants had implemented and maintained reasonable security and practices to protect her Private Information. With this belief in mind, Plaintiff Lopez provided her Private Information to Defendants in exchange for receiving healthcare services from Defendants.

16. In connection with providing healthcare services to Plaintiff Lopez, at all relevant times Defendants collected, stored, shared, and maintained Plaintiff Lopez's Private Information on their systems, including the systems involved in the Data Breach.

17. Had Plaintiff Lopez known that Defendants do not adequately protect the Private Information in their possession, she would not have agreed to provide Defendants with her Private Information or obtained healthcare services from Geisinger.

18. Plaintiff Lopez received a letter from Geisinger notifying her that her Private Information was accessed in the Data Breach.

19. Plaintiff Lopez has been the victim of identity theft as a result of the Data Breach. After the Data Breach, fraudulent charges appeared on Plaintiff Lopez's financial account, which forced her to replace her debit card. Due to the Data Breach, Plaintiff Lopez has also experienced an increase in the number of spam calls, texts, and emails she receives to the phone number and email address she provided to Defendants. Plaintiff Lopez spent time and effort researching the details of the Data Breach, monitoring her accounts for activity, and changing her account passwords in the wake of the Data Breach.

20. As a direct result of the Data Breach, Plaintiff Lopez has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft

and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive Private Information; deprivation of the value of her Private Information; lost time and money mitigating the effects of the Data Breach; and overpayment for services that did not include adequate data security.

Plaintiff Ralph Reviello

21. Plaintiff Reviello is a citizen and resident of the Commonwealth of Pennsylvania.

22. Plaintiff Reviello obtained healthcare services from Geisinger. As a condition of providing healthcare services to Plaintiff Reviello, Geisinger required Plaintiff Reviello to provide it with his Private Information. Geisinger in turn shared Plaintiff Reviello's Private Information with Nuance.

23. Plaintiff Reviello believed that Defendants had implemented and maintained reasonable security and practices to protect his Private Information. With this belief in mind, Plaintiff Reviello provided his Private Information to Defendants in exchange for receiving healthcare services from Defendants.

24. In connection with providing healthcare services to Plaintiff Reviello, at all relevant times Defendants collected, stored, shared, and maintained Plaintiff Reviello's Private Information on their systems, including the systems involved in the Data Breach.

25. Had Plaintiff Reviello known that Defendants do not adequately protect the Private Information in their possession, he would not have agreed to provide Defendants with his Private Information or obtained healthcare services from Defendants.

26. Plaintiff Reviello received a letter from Geisinger notifying him that his Private Information was accessed in the Data Breach.

27. Due to the data breach, Plaintiff Reviello has experienced an increase in the number of spam calls, texts, and emails he receives. Plaintiff Reviello spent time and effort contacting the three major credit bureaus and freezing his credit in the wake of the Data Breach.

28. As a direct result of the Data Breach, Plaintiff Reviello has suffered injury and damages including, inter alia, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive Private Information; deprivation of the value of his Private Information; lost time and money mitigating the effects of the Data Breach; and overpayment for services that did not include adequate data security.

Plaintiff Thomas Wilson

29. Plaintiff Wilson is a citizen and resident of the Commonwealth of Pennsylvania.

30. Plaintiff Wilson obtained healthcare services from Geisinger. As a condition of providing healthcare services to Plaintiff Wilson, Geisinger required Plaintiff Wilson to provide it with his Private Information. Geisinger in turn shared Plaintiff Wilson's Private Information with Nuance.

31. Plaintiff Wilson believed that Defendants had implemented and maintained reasonable security and practices to protect his Private Information. With this belief in mind, Plaintiff Wilson provided his Private Information to Defendants in exchange for receiving healthcare services from Defendants.

32. In connection with providing healthcare services to Plaintiff Wilson, at all relevant times Defendants collected, stored, shared, and maintained Plaintiff Wilson's Private Information on their systems, including the systems involved in the Data Breach.

33. Had Plaintiff Wilson known that Defendants do not adequately protect the Private Information in their possession, he would not have agreed to provide Defendants with his Private Information or obtained healthcare services from Defendants.

34. Plaintiff Wilson received a letter from Geisinger notifying him that his Private Information was accessed in the Data Breach.

35. Due to the data breach, Plaintiff Wilson suffered actual damages in the form of unauthorized medical bills and charges using his medical information. In or

around March 2024, Plaintiff Wilson received a bill for unauthorized medical expenses services from MedExpress. Plaintiff Wilson promptly contacted the healthcare facility to dispute the charge, indicating that Plaintiff Wilson did not engage in any recent visit with MedExpress as described by the fraudulent medical bill. Plaintiff Wilson's dispute was unsuccessful, forcing Plaintiff Wilson to pay the fraudulent medical bill, approximately $220.

36. In addition to unauthorized medical charges, Plaintiff Wilson has also experienced an increase in the number of spam calls and mail he receives. Plaintiff Wilson spent time and effort contacting reviewing his financial statements, speaking with his bank about the effects of the data breach, and taking efforts to replace impacted payment methods and updating automatic billing instructions that previously relied on impacted payment methods in the wake of the Data Breach.

37. As a direct result of the Data Breach, Plaintiff Wilson has suffered injury and damages including, inter alia, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive Private Information; deprivation of the value of his Private Information; lost time and money mitigating the effects of the Data Breach; and overpayment for services that did not include adequate data security.

Plaintiff Brenda Everett

38. Plaintiff Everett is a citizen and resident of the Commonwealth of Pennsylvania.

39. Plaintiff Everett obtained healthcare services from Geisinger. As a condition of providing healthcare services to Plaintiff Everett, Geisinger required Plaintiff Everett to provide it with her Private Information. Geisinger in turn shared Plaintiff Everett's Private Information with Nuance.

40. Plaintiff Everett believed that Defendants had implemented and maintained reasonable security and practices to protect her Private Information. With this belief in mind, Plaintiff Everett provided her Private Information to Defendants in exchange for receiving healthcare services from Defendants.

41. In connection with providing healthcare services to Plaintiff Everett, at all relevant times Defendants collected, stored, shared, and maintained Plaintiff Everett's Private Information on their systems, including the systems involved in the Data Breach.

42. Had Plaintiff Everett known that Defendants do not adequately protect the Private Information in their possession, she would not have agreed to provide Defendants with her Private Information or obtained healthcare services from Defendants.

43. Plaintiff Everett received a letter from Geisinger notifying her that her Private Information was accessed in the Data Breach.

44. Plaintiff Everett has been the victim of identity theft as a result of the Data Breach. After the Data Breach, several fraudulent charges appeared on Plaintiff Everett's financial accounts, forcing her to replace her cards. These fraudulent charges also caused her credit score to decrease by approximately 20 points. After learning of this fraud caused by the Data Breach, Plaintiff Everett spent approximately $30 per month for several months on a credit monitoring service in an effort to detect additional fraud.

45. Due to the data breach, Plaintiff Everett has also experienced a large increase in the number of spam calls, texts, and emails she receives. Plaintiff Everett spent time and effort researching the Data Breach and its potential consequences, checking her financial accounts, checking her credit score, and changing her passwords in the wake of the Data Breach. Plaintiff Everett was notified through her credit report that her information is now on the dark web.

46. As a direct result of the Data Breach, Plaintiff Everett has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive Private Information; deprivation of the value of her Private

Information; lost time and money mitigating the effects of the Data Breach; and overpayment for services that did not include adequate data security.

Plaintiff James Wierbowski

47. Plaintiff Wierbowski is a citizen and resident of Florida.

48. Plaintiff Wierbowski obtained healthcare services from Geisinger. As a condition of providing healthcare services to Plaintiff Wierbowski, Geisinger required Plaintiff Wierbowski to provide it with his Private Information. Geisinger in turn shared Plaintiff Wierbowski's Private Information with Nuance.

49. Plaintiff Wierbowski believed that Defendants had implemented and maintained reasonable security and practices to protect his Private Information. With this belief in mind, Plaintiff Wierbowski provided his Private Information to Defendants in exchange for receiving healthcare services from Defendants.

50. In connection with providing healthcare services to Plaintiff Wierbowski, at all relevant times Defendants collected, stored, shared, and maintained Plaintiff Wierbowski's Private Information on their systems, including the systems involved in the Data Breach.

51. Had Plaintiff Wierbowski known that Defendants do not adequately protect the Private Information in their possession, he would not have agreed to provide Defendants with his Private Information or obtained healthcare services from Defendants.

52. Plaintiff Wierbowski received a letter from Geisinger notifying him that his Private Information was accessed in the Data Breach.

53. Plaintiff Wierbowski was the victim of identity theft as a result of the Data Breach. After the Data Breach, fraudulent charges totaling more than $600 appeared on Plaintiff Wierbowski's financial accounts and PayPal account accounts, which forced him to replace both of his debit cards. Due to the data breach, Plaintiff Wierbowski has also experienced an increase in the number of spam texts and emails he receives, including spam emails containing his personal information. After the Data Breach, Plaintiff Wierbowski also had a fraudulent hard inquiry on his credit in February 2024. Plaintiff Wierbowski spent time and effort freezing his credit, changing passwords and login information, monitoring his financial accounts, and attempting to address and resolve the fraud he experienced in the wake of the Data Breach.

54. As a direct result of the Data Breach, Plaintiff Wierbowski has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive Private Information; deprivation of the value of his Private Information; lost time and money mitigating the effects of the Data Breach; and overpayment for services that did not include adequate data security.

Defendants

55. Defendant Geisinger Health is a Pennsylvania non-profit corporation with its headquarters located at 100 North Academy Avenue, Danville, Pennsylvania 17822.

56. Defendant Nuance Communications, Inc. is a Delaware corporation with its principal place of business located in Burlington, Massachusetts, and service of process address located at 84 State Street, Boston, Massachusetts, 02109 through its registered agent, Corporation Service Company.

JURISDICTION AND VENUE

57. This Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the aggregate matter in controversy exceeds $5,000,000, exclusive of interests and costs.

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

59. This Court has personal jurisdiction over Defendant Nuance Communications, Inc. because it regularly conducts business in this State, contracts to supply goods or services in this State, and has sufficient minimum contacts in this

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

60. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Geisinger is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

61. Defendant Geisinger is one of the nation's leading providers of value-based care, serving 1.2 million people in urban and rural communities across Pennsylvania.[5] Geisinger claims to generate $10 billion in annual revenues across 134 care sites, including 10 hospital campuses, and Geisinger Health Plan, with 600,000 members in commercial and government plans.[6]

62. Geisinger represents to its patients that it is "committed to protecting the privacy and confidentiality of its patients' and members' medical information."[7] Geisinger further acknowledges it has "an ethical obligation to use data

[5] *See Data Breach Notice*, *supra* n.3.
[6] *Id.*
[7] *For patients and members HIPAA notice of privacy practices*, GEISINGER, https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa (last accessed Mar. 13, 2025).

responsibly."[8] Geisinger acknowledges the "data in your electronic health record is linked to you in several ways (e.g., date of birth, address)."[9]

63. Geisinger assures its patients that "[e]very Geisinger employee is educated and trained in the appropriate use of patient and member data. Anyone accessing that data without authorization is subject to disciplinary action, including termination."[10]

64. Geisinger provides its patients with a Notice of Privacy Practices (the "Geisinger Privacy Policy") which "describes how medical information about [patients] may be used and disclosed."[11] Geisinger acknowledges it is "required to abide by the terms of this Notice."[12]

65. The Geisinger Privacy Policy states that "Geisinger may only use and disclose your PHI pursuant to an authorization, or as otherwise permitted or required by law."[13] Geisinger says it will only use its patients' Private Information for certain purposes, including treatment, healthcare operations, and billing and payment

---

[8] *Geisinger's principles for the ethical use of data*, GEISINGER, https://www.geisinger.org/about-geisinger/corporate/corporate-policies/geisingers-principles-for-the-ethical-use-of-data (last accessed Mar. 13, 2025)
[9] *Id.*
[10] *Id.*
[11] *Geisinger Notice of Privacy Practices*, GEISINGER, https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa/notice-of-privacy-practices-ghs (last accessed Mar. 13, 2025).
[12] *Id.*
[13] *Id.*

services.[14] Geisinger promises that "[o]ther uses and disclosures of your PHI not covered by the categories included in this Notice or applicable laws, rules or regulations will be made only with your written permission or authorization."[15]

66. Geisinger states, "[w]e are required by law to maintain the privacy and security of your PHI. We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[16]

67. Geisinger also states it complies "with all applicable federal and state laws and follow best practices to protect your data against loss, theft, unauthorized access, use, modification or disclosure."[17] Geisinger represents to its patients that it only shares personal information securely:

> Whenever we share data outside Geisinger, we do it securely and responsibly, following all laws and regulations. Through legal contracts, we hold our external partners to the same standards. Experts in law, ethics, privacy and technology make sure we only share data when it's legal and ethical to do so. And whenever possible, the data we share outside Geisinger is deidentified.[18]

68. In the regular course of its business, Geisinger collects and maintains the Private Information of its current and former patients. Geisinger required Plaintiffs and Class Members to provide their Private Information as a condition of providing healthcare services.

---

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Geisinger's principles for the ethical use of data*, *supra* n.8.
[18] *Id.*

69. Geisinger contracts with third-party vendors, including Defendant Nuance, for various services. According to Geisinger's Confidentiality for Vendors policy, "[Geisinger] take[s] the privacy and confidentiality of our patients, members and employees very seriously . . . Any vendor that has incidental exposure to PHI in the performance of their contractual duties is expected to follow all instructions from supervising Geisinger staff regarding confidentiality, and to keep such information strictly confidential. PHI should not be retained or utilized."[19]

70. Defendant Nuance provides healthcare technology services, including clinical solutions, diagnostic solutions, and revenue services.[20] On its website, Nuance claims its "AI-powered solutions" are used "by 77% of hospitals and 10,000 healthcare organizations worldwide" and "capture 300 million patient stories each year."[21]

---

[19] *See Confidentiality for Vendors*, GEISINGER, https://www.geisinger.org/-/media/OneGeisinger/pdfs/ghs/about-geisinger/vendor-relations/Confidentiality-for-Vendors.pdf?sc_lang=en&hash=B840CC881B4319B9DAFEDD4C9FF4C6A1 (last accessed Mar. 13, 2025).

[20] *See We are Nuance*, NUANCE, https://www.nuance.com/company-overview.html (last accessed Mar. 13, 2025).

[21] *Nuance*, BD. OF INNOVATION, https://healthcare.boardofinnovation.com/nuance/#:~:text=Clinical%20evidence,million%20patient%20stories%20each%20year. (last accessed Mar. 13, 2025).

71. In its regular course of business, Nuance collects personal data to deliver its products, conduct marketing, and run is business operations.[22] Nuance states, "We use the personal data that is processed within our Products, such as . . . medical data within medical data products . . . and any personal data contained within product usage data we collect, to deliver our Products sold to Nuance customers."[23]

72. Nuance represents that it "follow[s] generally accepted standards to protect the personal data submitted to us, both during transmission and once it is received."[24] It further represents it stores personal information on its secure servers.[25]

73. Nuance "collect[s] and use[s] consumer health data as reasonably necessary to provide you with the products you have requested or authorized."[26]

74. Nuance claims it "remain[s] firmly committed to helping our clients comply with their data protection requirements."[27] "Nuance assesses our process, procedures, and systems on a routine and regular basis to ensure that updates and

---

[22] *Nuance Privacy Statement*, NUANCE, https://www.nuance.com/about-us/company-policies/privacy-policies.html#collect (last accessed Mar. 13, 2025).
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *See Consumer Health Data Privacy Policy*, NUANCE, https://www.nuance.com/about-us/company-policies/privacy-policies/consumer-health-data-privacy-policy.html (last accessed Mar. 13, 2025).
[27] *Data Governance Program*, NUANCE, https://www.nuance.com/about-us/trust-center/privacy/data-governance.html (last accessed Mar. 13, 2025).

improvements are implemented to maintain our standards. assesses our process, procedures, and systems on a routine and regular basis to ensure that updates and improvements are implemented to maintain our standards.[28] Nuance claims it "conducts training on at least an annual basis, and more frequently as needed, to ensure workforce members are aware of their roles and responsibilities related to data governance."[29]

75. On its website, Nuance claims its patient data security approach includes, *inter alia*: "Assigning dedicated personnel to support privacy and security activities throughout the organization;" "Conducting regular HIPAA and data protection training;" "Restricting access as appropriate and necessary to information assets;" and "Managing authorized user access as well as ensuring employee accountability for any unauthorized use or disclosure."[30]

76. Nuance admits its "clients trust Nuance to deliver solutions that handle patient data responsibly."[31] Nuance purports to "remain firmly committed to helping our clients comply with their data protection requirements."[32]

---

[28] *Id.*
[29] *Id.*
[30] *Health Insurance Portability and Accountability Act (HIPAA)*, NUANCE, https://www.nuance.com/about-us/trust-center/privacy/hipaa.html (last accessed Mar. 13, 2025)
[31] *Data governance program*, *supra* n.27.
[32] *Id.*

77. Nuance promises it "remain[s] firmly committed to helping our clients comply with HIPAA."[33] Nuance claims to evaluate its "products and product environments for," *inter alia*, "Encryption of data;" "Restriction of physical access to production servers;" and "Configurable administrative controls that allow customers to: Manage access control and authorizations at a granular level," "Monitor and re-evaluate access rights," and "Obtain reporting and audit trails to account for both user and content activities audit trails to account for both user and content activities."[34]

78. Nuance claims, "[b]eyond the customer-facing side of our healthcare solutions, Nuance embraces a holistic approach to securing patient data within our custody. We maintain and regularly review policies and procedures for the consistent application of appropriate and necessary controls."[35] Nuance represents this includes, among other things, "[r]estricting access as appropriate and necessary to information assets;" "Managing authorized user access as well as ensuring employee accountability for any unauthorized use or disclosure;" and "Implementing cryptographic controls designed to protect the confidentiality, authenticity, and/or integrity of information."[36]

---

[33] *Health Insurance Portability and Accountability Act (HIPAA)*, *supra* n.30.
[34] *Id.*
[35] *Id.*
[36] *Id.*

79. Nuance states that its "responsibility with respect to data privacy—including access and controls—is shared" with its clients.[37]

80. Nuance promises it "maintains appropriate technical and organizational measures, through the implementation and enforcement" of certain policies, including:

> **Workforce Clearing, Training and Sanctions**
> All Nuance personnel are subject to background checks before access to restricted data is permitted. All personnel receive regular security training. Nuance has adopted policies and procedures to apply workforce sanctions to employees who fail to comply with Nuance security policies and procedures.
>
> * * *
>
> **Access**
> Nuance has located all equipment that stores Personal Data in controlled access areas. Nuance will only allow employees and contingent workers with a business purpose to have access to such controlled areas.
>
> * * *
>
> **Network Security**
> Nuance has implemented appropriate supplementary measures to protect Personal Data against the specific risks presented by the Services. All data is protected by encryption in transit over open, public networks. Data at rest is protected either by encryption or compensating security controls, which include pseudonymization, segmented networks, tiered architecture, firewalls with intrusion protection and anti-malware protections, and limiting of port access. Personal Data is only retained for the duration required for regulatory purposes, unless otherwise outlined by the Services.[38]

---

[37] *Id.*

[38] *Description of technical and organizational measures*, NUANCE (Aug. 1, 2023), https://www.nuance.com/about-us/terms-and-conditions/previous-

81. By creating and maintaining massive repositories of Private Information, Defendants have provided a particularly lucrative target for data thieves looking to obtain, misuse, or sell such data.

The Data Breach and Notice Letters

82. On or around November 29, 2023, Geisinger discovered that a former Nuance employee had accessed certain Geisinger patient information "two days after the employee had been terminated."[39]

83. Nuance did not revoke the employee's access to the health system's records upon termination, which allowed unauthorized access to the Private Information of more than a million patients.[40] Nuance determined the former employee may have accessed and taken information pertaining to more than one million Geisinger patients.[41]

---

versions/2023/TOMs-2023-0801.html. Nuance has an updated version of their description of the technical and organizational measures it takes to secure Private Information as of Mar. 10, 2025. *See* https://www.nuance.com/about-us/terms-and-conditions/data-processing-terms/TOMs.html. However, Plaintiff cites to the description in effect when the Data Breach occurred on or about November 29, 2023, though there are no differences in the relevant or material portions of the policies.

[39] *See Data Breach Notice, supra* n.3.

[40] Andrea Fox, *Geisinger alerts patients to data incident involving terminated Nuance employee*, HEALTHCARE IT NEWS (June 27, 2024), https://www.healthcareitnews.com/news/geisinger-alerts-patients-data-incident-involving-terminated-nuance-employee.

[41] *See Data Breach Notice, supra* n.3.

84. According to Nuance's investigation, the compromised data include a combination of dates of birth, addresses, admit and discharge or transfer codes, medical record numbers, race, gender, phone numbers, and facility name abbreviation.[42]

85. Although Geisinger discovered and notified Nuance of the Data Breach on or about November 29, 2023, Defendants did not begin to notify impacted breach victims about the Data Breach until approximately June 24, 2024, over six months after the Data Breach was discovered.[43] Defendants' failure to promptly notify Plaintiffs and Class Members that their Private Information was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that Private Information before Plaintiffs and Class Members could take affirmative steps to protect their sensitive information.

86. The compromised data contained Plaintiffs' and Class Members' Private Information that was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

87. Despite the ongoing and long-term risks for financial fraud and identity theft for victims of the Data Breach, Defendants do not offer sufficient identity

[42] *Id.*
[43] *See Data Breach Notice, supra* n.3.

protection services for the affected individuals. While Defendants provided instructions on how to obtain a credit report from the three credit reporting companies, and to place fraud alerts and credit or security freeze, this is far from sufficient, and placed the burden on the Data Breach victims to spend time and effort to sign up for these services provided, and future hardship to obtain credit.

88. Plaintiffs' and Class Members' Private Information was provided to Defendants, either directly or indirectly, with the reasonable expectation and mutual understanding that Defendants would comply with their obligation to keep such information confidential and secure from unauthorized access. Plaintiffs and Class Members are harmed by such failure.

89. Defendants also benefited directly from the Private Information provided by Plaintiffs and Class Members. As a healthcare provider and a third-party vendor, Defendants use the data they collect to perform their paid services for their customers.

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

The Criminal Action Against Max Vance

91. The former Nuance employee allegedly responsible for the Data Breach, Max Vance, was indicted by the federal government on January 30, 2025. *United States v. Vance*, No. 4:2024-cr-00015-MWB. Mr. Vance was charged with unauthorized access of a protected computer in violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(iii).

92. On January 30, 2024, the United States District Court for the Southern District of California—the district in which Mr. Vance was arrested—issued a detention order which held Mr. Vance without bail. According to the findings of fact that accompanied this order, Mr. Vance "possessed at his home + car [sic] numerous false ID cards w/ his photo + a variety of names" and also "possessed in his home blank ID docs + machines to create ID cards."[44] Significantly, there was also a "thumbdrive found hidden in [his] car with info from his former employer after he was fired," and Mr. Vance "used a variety of names during his law enforcement interactions."[45]

93. On March 7, 2024, after being transferred to this Court, Mr. Vance was arraigned and entered a plea of not guilty.

[44] *See United States v. Vance*, No. 4:2024-cr-00015-MWB, Docket Entry Nos. 12, 6.
[45] *Id.*

94. Jury selection and trial are currently scheduled to begin in Mr. Vance's criminal case on May 5, 2025, in Williamsport, Pennsylvania.

95. As noted above, Mr. Vance is accused of accessing the data at issue on November 29, 2024, which was "two days after he was fired by Nuance."[46]

Defendants Failed to Comply with Data Security Industry Standards

96. Experts studying cybersecurity have determined that "[d]ata breaches are both commonplace and costly in the medical industry" and that one of the two sectors within that industry that "sit at the top of the list of the highest average cost of a data breach" is healthcare.[47]

97. Defendants are aware of the importance of safeguarding Plaintiffs' and Class Members' Private Information, that by virtue of their business—as a healthcare organization and healthcare technology service provider—they place Plaintiffs' and Class Members' Private Information at risk of being targeted by cybercriminals.

98. Because Defendants failed to implement, maintain, and comply with necessary cybersecurity requirements, as a result, they were unable to protect

---

[46] John Beauge, *Suspect in Geisinger data breach case had false IDs, machines to make them: court order*, PENN LIVE (Jul. 10, 2024 1:05 AM), https://www.pennlive.com/news/2024/07/suspect-in-geisinger-data-breach-case-had-false-ids-machines-to-make-them-court-order.html (last accessed Mar. 13, 2025).

[47] Sue Poremba, *Cost of a data breach 2023: Pharmaceutical industry impacts*, SEC. INTEL. (Sept. 13, 2023), https://securityintelligence.com/articles/cost-of-a-data-breach-2023-pharmaceutical-industry/ (last accessed Mar. 13, 2025).

Plaintiffs' and Class Members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality.

99. As a proximate result of such failures, a former employee of Nuance gained unauthorized access to and acquired Plaintiffs' and Class Members' Private Information in the Data Breach without being stopped.

100. Defendants were unable to prevent the Data Breach and were unable to detect the unauthorized access to vast quantities of sensitive and protected files containing Plaintiffs' and Class Members' Private Information.

101. Commonly accepted data security standards among businesses and higher education institutions that store personal information, such as the Private Information involved here, include, but are not limited to:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for personal and financial information;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

102. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for Cybersecurity (Start with Security: A Guide for Business, (June 2015)) and protection of personal and financial information (Protecting Personal Information: A Guide for Business, (Oct. 2016)), which includes basic security standards applicable to all types of businesses and higher education institutions.

103. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses and higher education institutions must take to meet their data security obligations.

104. Because Defendants were entrusted with Plaintiffs' and Class Members' Private Information, they had and have a duty to keep the Private Information in their possession secure.

105. Plaintiffs and Class Members reasonably expect that when they entrusted their Private Information to Defendants, they would safeguard their information.

106. Despite Defendants' obligations, Defendants failed to appropriately monitor and maintain their data security systems in a meaningful way so as to prevent the Data Breach.

107. Had Defendants properly maintained their systems and adequately protected them, they could have prevented the Data Breach.

Defendants Violated their Common Law Duty of Reasonable Care

108. Defendants were aware of the importance of security in maintaining personal information (particularly sensitive information like the Private Information involved here), and the value consumers place on keeping their Private Information secure.

109. In addition to obligations imposed by federal and state law, Defendants owed and continue to owe a common law duty to Plaintiffs and Class Members—who entrusted Defendants with their Private Information—to exercise reasonable care in receiving, maintaining, and storing, the Private Information in Defendant's possession.

110. Defendants owed and continue to owe a duty to prevent Plaintiffs' and Class Members' Private Information from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. An essential part of Defendants' duties was (and is) the obligation to provide reasonable security consistent with current industry best practices and requirements, and to ensure information

technology systems and networks, in addition to the personnel responsible for those systems and networks, adequately protected and continue to protect Plaintiffs' and Class Members' Private Information.

111. Defendants owed a duty to Plaintiffs and Class Members, who entrusted Defendants with extremely sensitive Private Information, to design, maintain, and test the information technology systems that housed Plaintiffs' and Class Members' Private Information to ensure that the Private Information in Defendants' possession were adequately secured and protected.

112. Defendants owed a duty to Plaintiffs and Class Members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the Private Information stored in Defendants' systems. In addition, this duty also required Defendants to adequately train their employees and others with access to Plaintiffs' and Class Members' Private Information on the procedures and practices necessary to safeguard such sensitive information. This duty also required supervision, training, and compliance on Defendants' parts to ensure that they complied with creating, implementing, and maintaining reasonable data security practices and procedures sufficient to protect Plaintiffs' and Class Members' Private Information.

113. Defendants owed a duty to Plaintiffs and Class Members to implement processes that would enable Defendants to timely detect a breach or unauthorized

access of their information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

114. Defendants owed a duty to Plaintiffs and Class Members to disclose when and if their information technology systems and data security practices were not sufficiently adequate to protect and safeguard Plaintiffs' and Class Members' Private Information.

115. Thus, Defendants owed a duty to Plaintiffs and Class Members to timely disclose the fact that a data breach, resulting in unauthorized access to their Private Information, had occurred.

116. Defendants violated these duties. The Notice Letter states that Defendants became aware of the Data Breach on November 29, 2023. However, Plaintiffs and Class Members did not learn of the Data Breach until over six months later, and did not know whether their Private Information was impacted until Defendants sent out the notice letters in late June 2024. This demonstrates that Defendants did not properly implement measures designed to timely detect a data breach or unauthorized access of their information technology systems, as required to adequately safeguard Plaintiffs' and Class Members' Private Information.

117. Defendants also violated their duties to create, implement, and maintain reasonable data security practices and procedures sufficient to protect Plaintiffs' and Class Members' Private Information.

118. Defendants breached their obligations to Plaintiffs and Class Members and were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data and failed to prevent unauthorized access to Plaintiffs' and Class Members' Private Information. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and unauthorized access;

b. Failing to adequately protect patients' Private Information;

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

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to detect unauthorized ingress into its systems;

f. Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;

g. Failing to detect unauthorized exfiltration of the most sensitive data on its systems;

h. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

i. Failing to adhere to industry standards for cybersecurity as discussed above; and

j. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

119. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members Private Information by allowing cybercriminals to access their computer network which contained unsecured and unencrypted Private Information.

120. Had Defendants remedied the deficiencies in their information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

121. However, due to Defendants' failures, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendants.

Defendants Knew That Criminals Target Private Information

122. At all relevant times, Defendants knew or should have known that Plaintiffs' and all other Class Members' Private Information was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from unauthorized access that Defendants should have anticipated and guarded against.

123. Defendants' data security obligations were particularly important given the substantial increase in data breaches preceding the date of the Data Breach, which has been widely reported in the last few years.

124. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2025 report, Kroll found that "the healthcare industry was the most breached" in 2024.[48] The company found that 23% of the breaches that it handled responses for were from the healthcare industry, up from 18% in 2023.[49]

125. In the wake of the significant rise in data breaches, the Federal Trade Commission has also issued an abundance of guidance for companies and institutions that maintain individuals' Private Information.[50]

126. As a result of the notoriety of cyberattacks on systems like Defendants', several other government entities have also issued warnings to potential targets so that they may be alerted and prepared for a potential attack like the Data Breach.

127. The significant rise in data breaches has been a consistent problem for the past several years, providing Defendants sufficient time and notice to improve

[48] *Data Breach Outlook*, KROLL, https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2025 (last accessed Mar. 13, 2025).
[49] *See id*.
[50] *See, e.g.*, *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N., https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed Mar. 13, 2025).

the security of its systems and engage in stronger, more comprehensive cybersecurity practices.

128. Private Information is a valuable property right.[51] The value of Private Information as a commodity is measurable.[52] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[53] American companies are estimated to have spent over $19 billion acquiring consumers' personal data in 2018.[54] In fact, it is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[51] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFO. AND COMMC'N. TECH. 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

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

[53] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

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

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

130. Cybercriminals can use Private Information from one data breach in conjunction with other Private Information to commit identity fraud. For example, a cybercriminal might be able to use an address found in one data breach along with a credit card number in another one to make fraudulent credit card purchases.

131. Consumers place a high value on the privacy of their Private Information. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[55]

132. Given these factors, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has

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

thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

133. Therefore, Defendants clearly knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place, particularly given the nature of the Private Information stored in their unprotected files and the massive amount of Private Information they maintain.

Theft of Private Information Has Grave and Lasting Consequences for Victims

134. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's Private Information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victim's name, lock the victim out of their financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[56]

135. Identity thieves use stolen Private Information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[57] In

[56] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

[57] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). 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

addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[58]

136. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact on their credit.

137. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[59]

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

---

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." 12 C.F.R. § 1022.3(g).

[58] *See Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed Mar. 15, 2025).

[59] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Mar. 13, 2025).

Plaintiffs and Class Members Suffered Harm as a Result of the Data Breach

139. The ramifications of Defendants' failure to keep Private Information secure are long-lasting and severe. Victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.

140. Besides damage sustained in the event of identity theft, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues. The Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

141. Plaintiffs' and Class Members' Private Information was provided to Geisinger in conjunction with the type of work Geisinger performs as a healthcare provider. Geisinger, in turn, provided Plaintiffs' and Class Members' Private Information to Nuance for the purpose of using their services to help provide healthcare to Plaintiffs and Class Members. In requesting and maintaining Plaintiffs' and Class Members' Private Information, Defendants promised, and undertook a duty, to act reasonably in their handling of Plaintiffs' and Class Members' Private Information. Defendants, however, did not take proper care of Plaintiffs' and Class Members' Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Defendants' inadequate data security measures.

142. As a result of Defendants' conduct and failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Private Information, which allowed the Data Breach to occur, Plaintiffs' and Class Members' Private Information has been and is now in the hands of unauthorized individuals and third parties, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals.

143. Plaintiffs and Class Members greatly value their privacy, especially their highly sensitive Private Information. They would not have entrusted Defendants with this highly sensitive information had they known that Defendants would negligently fail to adequately protect their Private Information. Indeed, Plaintiffs and Class Members provided Defendants with this highly sensitive information with the expectation that Defendants would keep their Private Information secure and inaccessible from unauthorized parties.

144. As a result of Defendants' failure to implement and follow even the most basic security procedures, Plaintiffs and all other Class Members have suffered injury and damages, including, but not limited to (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their

Private Information, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

CLASS ALLEGATIONS

145. This action is brought and may be properly maintained as a class action pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

146. Plaintiffs bring this action on behalf of themselves and all members of the following Nationwide Class of similarly situated persons:

> All residents of the United States whose Private Information was compromised in the Data Breach.

147. In the alternative to the Nationwide Class, Plaintiffs seek to represent each of the following two state-wide classes:

> All residents of Pennsylvania whose Private Information was compromised in the Data Breach (the "Pennsylvania Class").
>
> All residents of Florida whose Private Information was compromised in the Data Breach (the "Florida Class").

148. The Nationwide Class, Pennsylvania Class, and Florida Class will be collectively referred to herein as the "Class."

149. Plaintiffs reserve the right to amend the above definition or to propose other or additional classes in subsequent pleadings and/or motions for class certification.

150. Plaintiffs are members of the Class.

151. Excluded from the Class are Defendants, their respective affiliates, parents, subsidiaries, officers, agents, directors, the judge(s) presiding over this matter, and the clerks of said judge(s).

152. This action seeks both injunctive relief and damages.

153. Plaintiffs and the Class satisfy the requirements for class certification for the following reasons:

154. **Numerosity of the Class.** The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. Upon information and belief, there are over one million Class Members in the Class. The exact number and identity of Class Members is readily identifiable in Defendants' records, which will be a subject of discovery.

155. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendants' data security measures prior to the Data Breach met the requirements of relevant laws;

b. Whether Defendants' data security measures prior to the Data Breach met industry standards;

c. Whether Defendants owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

d. Whether Defendants breached their duty to Plaintiffs and Class Members to safeguard their Private Information;

e. Whether Defendants failed to provide timely and adequate notice of the Data Breach to Plaintiffs and Class Members;

f. Whether Plaintiffs' and Class Members' Private Information was compromised in the Data Breach;

g. Whether Plaintiffs and Class Members are entitled to injunctive relief; and

h. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendants' conduct.

156. **Typicality.** The claims or defenses of Plaintiffs are typical of the claims or defenses of the proposed Class because Plaintiffs' claims are based upon the same legal theories and violations of law. Plaintiffs and Class Members all had their Private Information stolen in the Data Breach. Plaintiffs' grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendants.

157. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent the Class on whose behalf this action is prosecuted. Their interests do not conflict with the interests of the Class.

158. Plaintiffs and Interim Co-Lead Class Counsel ("Class Counsel") are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint. In particular, Class Counsel have respectively been appointed as lead counsel in several complex class actions across

the country and has secured numerous favorable judgments in favor of their clients, including in cases involving data breaches. Class Counsel are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class Members. Finally, Class Counsel possess the financial resources necessary to ensure that a lack of financial capacity will not hamper the litigation and is willing to absorb the costs of the litigation.

159. **Predominance.** The common issues identified above arising from Defendants' conduct predominate over any issues affecting only individual Class Members. The common issues hinge on Defendants' common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

160. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large number of injured persons, to keep the courts from becoming paralyzed by a multitude of repetitive cases, and to reduce transaction costs so that the injured Class Members can obtain the most compensation possible.

161. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which, in any event, might cause inconsistent results.

b. When the liability of Defendants have been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendants to all Class Members, in terms of monetary damages due and terms of equitable relief, can be determined in this single proceeding rather than in multiple individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendants, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only customers of Defendants, the legal and factual issues are narrow and easily defined, and the Class Membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendants' records, such that direct notice to the Class Members would be appropriate.

162. **Injunctive relief.** Defendants have acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final injunctive or equitable relief on a class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class Against Both Defendants)

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

164. To perform its healthcare services, Defendant Geisinger collected Plaintiffs' and Class Members' Private Information, and provided the Private Information to Defendant Nuance for the purpose of using Nuance's third-party software services.

165. By collecting and storing their Private Information and using it for commercial gain, at all times relevant, Defendants owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting their Private Information in their possession, custody, or control.

166. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with statutory and industry standards and their representations, and to ensure that their systems and networks and the personnel responsible for them adequately protected the Private Information.

167. Defendants knew the risks of collecting and storing Plaintiffs' and all other Class Members' Private Information and the importance of maintaining secure systems. Defendants knew of the many data breaches that targeted companies that store Private Information in recent years.

168. Given the nature of Defendants' businesses, the sensitivity and value of the Private Information they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities in their systems and prevented the Data Breach from occurring.

169. Defendants breached these duties by failing to, or sharing Private Information with third parties who failed to, exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to them—including Plaintiffs' and Class Members' Private Information.

170. Plaintiffs and Class Members are a well-defined, foreseeable, and probable group of customers that Defendants were aware, or should have been aware, could be injured by inadequate data security measures.

171. Plaintiffs and Class Members have no ability to protect their Private Information that was or remains in Defendants' possession.

172. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to, or sharing Private Information with third parties that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized access, release, disclosure, and dissemination of Plaintiffs' and Class Members' Private Information to unauthorized individuals.

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

174. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to failing to adequately protect Plaintiffs' and Class Members' Private Information and failing to provide them with timely notice that their Private Information had been compromised.

175. Neither Plaintiffs nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

176. By failing to provide timely and complete notification of the Data Breach to Plaintiffs and Class Members, Defendants prevented them from

proactively taking steps to secure their Private Information and mitigate the associated threats.

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

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class Against Both Defendants)

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

179. Defendants had duties by statute to ensure that all sensitive information they collected and stored was secure and to maintain adequate and commercially

reasonable data security practices to ensure the protection of Plaintiffs' and Class Members' Private Information.

180. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

181. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure Private Information.

182. The FTC has published numerous guides for businesses that highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication establishing cybersecurity guidelines for businesses, which makes thorough recommendations, including, but not limited to, for businesses to protect the personal customer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer

networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[60]

183. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA. Orders resulting from these actions further clarify the measures businesses such as Defendants must take to meet their data security obligations and effectively put Defendants on notice of these standards.

184. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all Class Members' Private Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtain and store and the foreseeable consequences of a data breach involving Private Information, including, specifically, the substantial damages that would result to Plaintiffs and other Class Members.

185. Defendants' violation of HIPAA Privacy and Security Rules and the FTCA constitutes negligence per se.

---

[60] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N. (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

186. Plaintiffs and Class Members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA was intended to protect.

187. The harm occurring as a result of the Data Breach is the type of harm against which HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard.

188. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' Private Information to unauthorized individuals.

189. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Defendants' violation of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class Members have suffered (and will continue to suffer) damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper

disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

190. Defendants' violation of the HIPAA Privacy and Security Rules and FTCA constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect a group to which Plaintiffs belongs and to prevent the type of harm that resulted from the Data Breach.

191. Defendants owed a duty of care to Plaintiffs and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

192. It was foreseeable that Defendants' failure to use reasonable measures to protect Private Information and provide timely notice of the Data Breach would result in injury to Plaintiffs and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Class were reasonably foreseeable.

193. It was therefore foreseeable that the failure to adequately safeguard Private Information would result in one or more of the following injuries to Plaintiffs and the members of the proposed Class: ongoing, imminent, and certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class Against Defendant Geisinger)

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

195. Plaintiffs' and Class Members' Private Information was provided to Geisinger in confidence, believing that Geisinger would protect that information. Plaintiffs and Class Members would not have provided Geisinger with this information had they known it would not be adequately protected. Geisinger's acceptance and storage of Plaintiffs' and Class Members' Private Information

created a fiduciary relationship between Geisinger and Plaintiffs and Class Members.

196. In light of this relationship, Geisinger has a fiduciary duty to act for the benefit of its patients, including Plaintiffs and Class Members, upon matters within the scope of their relationship, which includes safeguarding and protecting Plaintiffs' and Class Members' Private Information.

197. Geisinger breached that duty by failing to, or sharing Private Information with third parties that failed to, properly protect the integrity of the system containing Plaintiffs' and Class Members' Private Information and otherwise failing to safeguard Plaintiffs' and Class Members' Private Information that it collected.

198. As a direct and proximate result of Geisinger's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury, including, but not limited to (i) a substantially increased and imminent risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) the improper compromise, publication, and theft of their Private Information; (iii) deprivation of the value of their Private Information, for which there is a well-established national and international market; (iv) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity

theft they face and will continue to face; and (v) the continued risk to their Private Information which remains in Geisinger's possession.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class Against both Defendants)

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

200. In connection with receiving healthcare services, Plaintiffs and Class Members entered into implied contracts with Geisinger.

201. Pursuant to these implied contracts, Plaintiffs and Class Members paid money to Geisinger, whether directly or through their insurers, and provided Geisinger with their Private Information. In exchange, Geisinger agreed to, among other things, and Plaintiffs and Class Members understood that Geisinger would: (1) provide healthcare services to Plaintiffs and Class Members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' Private Information; and (3) protect Plaintiffs' and Class Members Private Information in compliance with federal and state laws and regulations and industry standards.

202. The protection of Private Information was a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and Geisinger, on the other hand. Had Plaintiffs and Class Members known that

Geisinger would not adequately protect their Private Information, they would not have sought healthcare services from Geisinger or agreed to provide Geisinger with their Private Information.

203. Plaintiffs and Class Members performed their obligations under the implied contract when they provided Geisinger with their Private Information and paid—directly or through their insurers—for healthcare services from Geisinger.

204. Geisinger breached its obligations under the implied contracts with Plaintiffs and Class Members in failing to, or sharing Private Information with third parties that failed to, implement and maintain reasonable security measures to protect and secure their Private Information and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' Private Information in a manner that complies with applicable laws, regulations, and industry standards.

205. Geisinger's breach of its obligations of the implied contracts with Plaintiffs and Class Members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class Members have suffered from the Data Breach.

206. Plaintiffs and all other Class Members were damaged by Geisinger's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk or imminent threat of identity theft and medical identity

theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Private Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Private Information has been breached; (v) they were deprived of the value of their Private Information, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Class Against Both Defendants)

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

208. Defendant Nuance entered into a written contract with Defendant Geisinger to perform services that include, but are not limited to, computer software technology services.

209. This contract was made in part for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contract entered into between Defendants. Indeed, Defendants knew that if they were to breach the third-party beneficiary contract, Geisinger's patients, including

Plaintiffs and Class Members, would be harmed by, among other things, fraudulent misuse of their Private Information.

210. It was intended by Defendant Nuance at the time the contracts were made that Defendant Nuance would assume a direct obligation to protect Plaintiffs' and the Class's Private Information.

211. It was also intended by Defendant Nuance that the performance under the contract would necessarily and directly benefit Plaintiffs and the Class, in that Nuance would provide technological services to aid Geisinger in utilizing Plaintiffs' and Class Members' Private Information in the course of providing healthcare services to Plaintiffs and Class Members.

212. Both Defendants breached their obligations under this contract, to which Plaintiffs and Class Members are intended beneficiaries, which directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class Members have suffered.

213. As a direct and proximate result of Defendants' breach of this third-party beneficiary contract, Plaintiffs and all other Class Members suffered and will continue to suffer damages, because (i) they face a substantially increased and imminent risk of identity theft or fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) their Private Information was improperly disclosed to unauthorized individuals; (iii) the

confidentiality of their Private Information has been breached; (iv) they were deprived of the value of their Private Information, for which there is a well-established national and international market; and (v) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and fraud they face and will continue to face.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class Against Both Defendants)

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

215. Plaintiffs bring this claim, on behalf of themselves and the Class, in the alternative to all other claims and remedies at law.

216. Plaintiffs and Class Members conferred a monetary benefit on Defendant Geisinger in the form of (1) monies paid for healthcare services by Plaintiffs and Class Members (either directly or through their insurance), and (2) the provision of Plaintiffs' and Class Members' valuable Private Information. Indeed, upon acquiring the Private Information, Defendant Geisinger was then able to charge money for its services and utilize the Private Information for several purposes, including but not limited to, providing its healthcare services, billing, and contacting

patients. The Private Information was thus used to facilitate payment and generate additional revenue for Defendant Geisinger.

217. Defendant Nuance was conferred a monetary benefit upon by collecting Plaintiffs' and Class Members' Private Information, in the forms of (1) monies paid for services by Geisinger, and (2) the provision of Plaintiffs' and Class Members' valuable Private Information. Indeed, upon acquiring the Private Information, Defendant Nuance was then able to charge money for its services from Geisinger and utilize the Private Information. The Private Information was thus used to facilitate payment and generate additional revenue for Defendant Nuance.

218. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

219. Upon information and belief, Defendants, like most other corporate entities, funds their data security measures entirely from their general revenue, which includes money paid by Plaintiffs and Class Members.

220. As such, a portion of the money paid to Defendants, directly or indirectly, should have been used to provide a reasonable level of data security.

221. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to protect the Private Information they collect.

222. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants avoided their data security obligations at the expense of Plaintiffs and Class Members by utilizing less expensive and less effective security measures.

223. As a direct and proximate result of Defendants' failure to provide the requisite security, Plaintiffs and Class Members were harmed as described herein.

224. Defendants should not be permitted to retain the money profited by collecting Private Information of Plaintiffs and Class Members because Defendants failed to adequately implement the data privacy and security procedures mandated by federal, state, and local laws and industry standards.

225. Defendants should be compelled to provide for the benefit of Plaintiffs and Class Members all unlawful proceeds received by them as a result of their conduct and the resulting Data Breach alleged herein.

COUNT VII
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class Against Both Defendants)

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

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

228. Defendants owe a duty of care to Plaintiffs and Class Members that require them to adequately secure Plaintiffs' and Class Members' Private Information.

229. Defendants still possess the Private Information of Plaintiffs and Class Members.

230. Defendants have not satisfied their contractual obligations and legal duties to Plaintiffs and Class Members.

231. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendants' failure to address the security failings that led to such exposure.

232. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the Data Breach to meet Defendants' contractual obligations and legal duties.

233. Plaintiffs, therefore, seek a declaration stating that (1) Defendants' existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their

contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants maintain rigorous hiring practices and training for all employees who have access to Private Information;

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

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

d. Ordering that Defendants audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

e. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for provision of their services;

f. Ordering that Defendants conduct regular database scanning and security checks; and

g. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, patients Private Information.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendants as follows:

A. Certifying the Class as requested herein and appointing the named Plaintiffs as Class representatives and the undersigned counsel as Class Counsel;

B. Requiring that Defendants pay for notifying the members of the Class of the pendency of this suit;

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

D. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard Private Information and to provide or extend additional credit monitoring services and similar services to protect against all types of identity theft and medical identity theft.

E. Awarding Plaintiffs and the Class prejudgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable, together with their costs and disbursements of this action; and

G. Awarding Plaintiffs and the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Consolidated Class Action Complaint so triable.

Date: March 17, 2025

Respectfully submitted,

/s/ *Benjamin F. Johns*
Benjamin F. Johns (PA ID 201373)
Samantha E. Holbrook (PA ID 311829)
SHUB JOHNS & HOLBROOK LLP
200 Barr Harbor Dr., Suite 400
Conshohocken, PA 19428
Tel: 610-477-8380
bjohns@shublawyers.com
sholbrook@shublawyers.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Interim Co-Lead Counsel for Plaintiffs

Andrew W. Ferich
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087

Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Scott Edward Cole*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
sec@colevannote.com

Todd S. Garber**
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com

Jeffrey M. Ostrow**
Kenneth Grunfeld
KOPELOWITZ OSTROW P.A.
65 Overhill Road
Bala Cynwyd, PA 19004
Telephone: (954) 525-4100
ostrow@kolawyers.com
grunfeld@kolawyers.com

Counsel for Plaintiffs

*Admitted *pro hac vice*
***Pro hac vice* forthcoming

CERTIFICATE OF SERVICE

I, Benjamin F. Johns, hereby certify that I caused the foregoing Consolidated Class Action Complaint to be filed on this 17th day of March 2025, thereby causing it to be electronically served via CM/ECF upon all counsel of record.

/s/ Benjamin F. Johns
Benjamin F. Johns