UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
EASTERN DISTRICT

JUAN SALAS, individually, and on behalf of all others similarly situated, **Plaintiff,** **vs.** **NUANCE COMMUNICATIONS, INC.,** **Defendant.**	**Case No. _____** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Juan Salas, individually, and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant, Nuance Communications, Inc., ("Defendant" or "Nuance"), and alleges as follows.

INTRODUCTION

1. Plaintiff brings this class action against Nuance for its failure to secure and safeguard the sensitive information of over one million people that it was entrusted to safeguard. As a result of its failure to do so as described below, the following types of personally identifiable information are now in the hands of criminal hackers: Names, details about radiology studies received, including a description of the studies, dates of service, providers, facility names, and study identifiers. According to the Maine Attorney General Office, the breach also included names and other personal identifiers, combined with Social Security numbers, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health

Insurance Portability and Accountability Act of 1996 ("HIPAA")[1].

2. Nuance offers artificial intelligence solutions to document patient visits around the world.[2] Nuance works with clinicians, radiologists, and care teams to capture clinical informational and suggest decision making strategies.[3] Nuance services are used by "77% of hospitals and 10,000 healthcare organizations worldwide."[4] Nuance states "we protect user's privacy by taking steps such as de-identifying the data, requiring non-disclosure agreements with relevant vendors and their employees, and requiring that employees and vendors meet high privacy standards."[5]

3. According to Nuance's notice letter, the software of one of its third-party vendors "was recently the victim of a security incident, which impacted some of your personal information" between May 28 and May 29, 2023 ("Data Breach"). On July 10, 2023, Nuance confirmed the personal information was stolen. And on August 8, 2023, Nuance notified the Plaintiff's healthcare provider about the incident. Yet it was not until September 22, 2023, that Nuance began notifying its users, including Plaintiff, that their data was stolen.

4. Nuance owed a non-delegable duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Private Information against unauthorized access and disclosure. It also had an obligation to ensure that any vendor or third party it selected to offload the sensitive information it was entrusted with would take reasonable measures to safeguard that data.

5. As a result of Nuance's inadequate vendor screening and security measures, and

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/66187ace-3687-41c3-ab65-33363ae1f399.shtml (las visited Oct. 2, 2023).
[2] https://www.nuance.com/index.html (last visited Oct. 2, 2023).
[3] *Id.*
[4] *Id.*
[5] https://www.nuance.com/about-us/company-policies/privacy-policies.html (last visited Oct. 2, 2023).

breach of its legal duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' Private Information was accessed and stolen by an unspecified actor. Nuance permitted Plaintiff's and Class members' Private Information to be held in unencrypted form despite the heightened sensitivity of such Private Information.

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

7. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

8. Plaintiff and Class members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity

costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of their Private Information; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

9. Plaintiff, on behalf of himself and all other Class members, asserts claims herein against Nuance for negligence, negligence *per se*, breach of fiduciary duty, breach of third-party beneficiary contract, and, alternatively, unjust enrichment.

10. Plaintiff and Class members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

11. Plaintiff is a resident and citizen of Durham, North Carolina. Plaintiff received a letter from Nuance regarding the Data Breach, dated September 22, 2023 ("Notice"). The Notice states: "the personal information involved may have included your name and details about radiology studies you received, including a description of the study, date of service, provider, and facility name, and study identifiers."

12. Plaintiff takes great care to protect his Private Information. Had Plaintiff known that Nuance would not adequately protect the Private Information entrusted to it, he would not have accepted Nuance's services or agreed to provide Nuance with his Private Information.

13. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a present and continuing risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive Private Information; and deprivation of the value of his Private Information.

14. Defendant is a Delaware corporation with its principal place of business located at 1 Wayside Road, Burlington, MA 01803.

JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of Class members exceeds 100, many of whom have different citizenship from Nuance. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

16. This Court has personal jurisdiction over Nuance because its principal place of business is in this District.

17. Venue is proper in this District because Nuance's principal place of business is in this District and a significant amount of the events leading to Plaintiff's causes of action occurred in this District.

FACTUAL ALLEGATIONS

Overview of Nuance's Data Breach

18. Nuance, formally operating as ScanSoft, Inc., was founded in 1992 on the premise of delivering imaging solutions that simplified converting and managing information as it

transferred from paper to electronic form.[6] It is now one of the nation's largest computer software technology corporations. Nuance was acquired by Microsoft, Inc. on March 4, 2022.[7]

19. In the course of its ordinary business operations, Nuance is entrusted with safeguarding the sensitive Private Information of its customers. According to Nuance, it uses software made by Progress Software Corporation, a third-party vendor, called MOVEit Transfer, to exchange audit logs pertaining to radiology images among healthcare providers.

20. As alleged above, Nuance's vendor's software was hacked between May 28 and May 29, 2023.

21. Nuance stated that, upon learning of the breach, "we immediately took steps to secure the servers running the MOVEit Transfer application and worked with cybersecurity experts and legal counsel to conduct a comprehensive investigation of the incident and notify affected individuals."

Nuance Knew that Criminals Target Private Information

22. Nuance knew that the sensitive personal data with which it was entrusted would be a lucrative target for hackers. Despite such knowledge, Nuance and its vendor both failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' Private Information from cyber-attacks that Nuance should have anticipated and guarded against.

23. It is well known amongst companies that store sensitive PII that sensitive

---

[6]https://www.sec.gov/Archives/edgar/data/1002517/000095013505006971/b58154nce10vk.htm#:~:text=Nuance%20was%20incorporated%20in%201992,our%20ticker%20symbol%20to%20NUAN. (last visited Oct. 2, 2023).

[7] https://news.microsoft.com/2022/03/04/microsoft-completes-acquisition-of-nuance-ushering-in-new-era-of-outcomes-based-ai/#:~:text=Strategic%2C%20highly%20complementary%20acquisition%20accelerates,acquisition%20of%20Nuance%20Communications%20Inc. (last visited Oct. 2, 2023).

information—such as the Social Security numbers and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[8]

24. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[9] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[10]

25. PII and PHI are valuable property rights.[11] Their value as a commodity is measurable.[12] "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."[13] American companies are estimated to have spent over $19 billion on acquiring

[8] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[9] *See* PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last visited Oct. 2, 2023).
[10] *See id*.
[11] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[12] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.
[13] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

personal data of consumers in 2018.[14] 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.

26. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, Private Information, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated, becoming more valuable to thieves and more damaging to victims.

27. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[15] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[16]

28. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[17] According to a report released by the Federal Bureau of

[14] *See* IAB Data Center of Excellence, *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*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.
[15] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[16] *Id.*
[17] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[18]

29. Criminals can use stolen PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[19] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[20]

30. Consumers place a high value on the privacy of that data, as they should. 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."[21]

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

Defendant Fails to Comply with FTC Guidelines

32. The Federal Trade Commission ("FTC") has promulgated numerous guides for

[18] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[19] *What Happens to Stolen Healthcare Data*, *supra* note 20.
[20] *Id.*
[21] 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.

businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

33. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[22]

34. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[23]

35. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

[22] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 2, 2023).
[23] *Id.*

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 ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

37. These FTC enforcement actions include actions against healthcare entities, like Defendant.

38. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

39. Defendant failed to properly implement basic data security practices.

40. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff and Class members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

41. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its customers, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Fails to Comply with HIPAA Guidelines

42. Defendant is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

43. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[24] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

45. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

46. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

47. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

48. HIPAA's Security Rule requires Defendant to do the following:

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

a. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

49. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

50. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

51. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable

delay and ***in no case later than 60 days following discovery of the breach***."[25]

52. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

53. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

54. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[26] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health &

[25] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).
[26] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Oct. 3, 2023).

Human Services, Guidance on Risk Analysis.[27]

Defendant Fails to Comply with Industry Standards

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

56. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

57. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protecting physical security systems; protecting against any possible communication system; and training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failing to train staff.

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

[27] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Oct. 3, 2023).

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

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

Theft of Private Information Has Grave and Lasting Consequences for Victims

60. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[28]

61. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[29] Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a

[28] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Oct. 2, 2023).

[29] 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 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).

tax return, and applying for government benefits.[30]

62. With access to an individual's Private Information, criminals can do more than just empty a victim's bank account—they can also commit all manners of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[31]

63. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[32]

64. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their Social Security number, and a new Social Security number will not be provided until after the harm has already been suffered by the victim.

65. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other Private Information (*e.g.*, names, addresses, and dates of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data

---

[30] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[31] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Oct. 2, 2023).

[32] *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited Oct. 2, 2023).

security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[33]

66. Theft of Private Information is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[34] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[35] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use Private Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [36] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[37]

67. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

---

[33] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[34] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[35] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* note 23.

[36] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Oct. 2, 2023).

[37] *Id*.

- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime. For example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; and victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[38]

68. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[39]

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

[38] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* note 39.
[39] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

Common Injuries and Damages

70. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class members has materialized and is present and continuing, and Plaintiff and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' Private Information.

The Data Breach Increases Victims' Risk Of Identity Theft

71. Plaintiff and Class members are at a heightened risk of identity theft for their lifetimes.

72. The unencrypted Private Information of Class members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class members.

73. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other

criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

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

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

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

[40] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on Oct. 2, 2023).

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

78. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

79. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the Data Breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class members.

80. Thus, even if certain information (such as driver's license numbers) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

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

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

82. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim

of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

83. Thus, due to the present and continuing risk of identity theft, Plaintiff and Class members must, as Defendant's Notice encourages, stay alert and check their accounts for fraudulent activity for the rest of their lives to mitigate the risk of identity theft.

84. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach as well as monitoring their accounts for any indication of fraudulent activity, which may take years to detect.

85. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[41]

86. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[42]

---

[41] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[42] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Oct. 2, 2023).

Future Cost Of Credit And Identity Theft Monitoring Is Reasonable And Necessary

87. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, upon information and belief, entire batches of stolen information have been placed on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

88. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

89. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[43] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

90. Consequently, Plaintiff and Class members are at a present and continuous risk of fraud and identity theft for the remainder of their lives.

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

91. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor to protect Class members from the risk of identity theft that arose from the Data Breach. This is a future cost that Plaintiff and Class members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss Of The Benefit Of The Bargain

92. Furthermore, Defendant's poor data security deprived Plaintiff and Class members of the benefit of their bargain. When agreeing to pay Defendant for products and/or services, reasonable consumers, including Plaintiff and Class members, understood and expected that they were, in part, paying for the service that provided the necessary data security to protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Experience

93. Plaintiff is a current customer of Defendant. Defendant provides solutions to share radiology documentation among Plaintiff's healthcare providers.

94. As a condition to utilize Defendant's services, Plaintiff was required to provide his Private Information, directly or indirectly, to Defendant.

95. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

96. At the time of the Data Breach—on or about May 28, 2023, and May 29, 2023—

Defendant retained Plaintiff's Private Information in its system.

97. Plaintiff received the Notice, by U.S. mail, from Defendant, dated September 22, 2023. According to the Notice, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his name and details about radiology studies he received, including a description of the study, date of service, provider and facility name, and study identifiers. Although Nuance did not notify the Plaintiff about his Social Security information being disclosed, Maine's Attorney General Office linked the hack to a Social Security data breach.[44]

98. Upon receiving the Notice from Defendant, Plaintiff has spent significant time dealing with the consequences of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice as well as monitoring his accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

99. Subsequent to the Data Breach, Plaintiff has suffered numerous, substantial injuries including, but not limited to: (i) lost or diminished value of his Private Information; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) invasion of privacy; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to his Private Information, which: (a) remains

[44] https://apps.web.maine.gov/online/aeviewer/ME/40/66187ace-3687-41c3-ab65-33363ae1f399.shtml (las visited Oct. 2, 2023).

unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

100. Plaintiff also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number and PHI, being in the hands of criminals.

101. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

102. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

103. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

CLASS ALLEGATIONS

105. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and 23(b)(3).

106. Plaintiff brings this action individually, and on behalf of all members of the following Class of similarly situated persons:

> All persons whose PII or PHI was compromised in the Data Breach by unauthorized persons, including all persons who were sent a Notice of the Data Breach.

107. Excluded from the Class are Nuance and its affiliates, parents, subsidiaries, officers,

agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

108. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

109. The members of the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. Nuance sent its notice letter to over 1,200,000 users who were affected by the breach.[45]

110. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Nuance had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' Private Information from unauthorized access and disclosure;

b. Whether Nuance had duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

c. Whether Nuance failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' Private Information;

d. Whether Nuance breached a fiduciary duty to Plaintiff's and Class members when it failed to protect their Private Information;

e. Whether Defendant entered into contract(s) with third parties expressly for the benefit of Plaintiff and Class members;

f. Whether Nuance was unjustly enriched when it did not provide adequate data security in return for the benefit Plaintiff and Class members provided;

g. Whether Nuance breached its duties to protect Plaintiff's and Class members' Private Information; and

[45] https://healthitsecurity.com/news/nuance-communications-notifies-1.2m-individuals-of-data-breach (last visited Oct. 2, 2023)

h. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

111. Nuance engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that predominate in this action.

112. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his Private Information compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Nuance, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

113. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

114. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Nuance, so it would be impracticable for Class members to individually seek redress from Nuance's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for

inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

115. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

116. Defendant requires its customers, including Plaintiff and Class members, to submit non-public Private Information in the ordinary course of providing its services.

117. Defendant gathered and stored the Private Information of Plaintiff and Class members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

118. Plaintiff and Class members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

119. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

120. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Plaintiff and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to

implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

121. Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

122. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

123. Defendant's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Defendant and its customers and its clients' plan members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of being Defendant's customer.

124. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

125. Thus, Defendant was subject to an "independent duty," untethered to any

contract between Defendant and Plaintiff or the Class.

126. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' Private Information it was no longer required to retain pursuant to regulations.

127. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

128. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

129. Defendant breached its duties, pursuant to the FTCA, HIPAA, and other applicable standards, and thus were negligent by failing to use reasonable measures to protect Plaintiff and Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Plaintiff and Class members' Private Information;

e. Failing to detect in a timely manner that Plaintiff and Class members' Private Information had been compromised;

f. Failing to remove former customers' Private Information it was no longer required to retain pursuant to regulations; and

g. Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that it could take appropriate steps to mitigate the potential for identity theft and other damages.

130. Defendant violated Section 5 of the FTCA and HPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

131. Plaintiff and the Class are within the class of persons that the FTCA and HIPAA were intended to protect.

132. The harm that occurred as a result of the Data Breach is the type of harm the FTCA and HIPAA were intended to guard against.

133. Defendant's violation of Section 5 of the FTCA and HIPAA constitutes negligence.

134. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

135. A breach of security, unauthorized access, and resulting injury to Plaintiff and

the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

136. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

137. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

138. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

139. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

140. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

141. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

142. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put

in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

143. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

144. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

145. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

146. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of their Private Information; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to

undertake appropriate and adequate measures to protect their Private Information.

147. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

148. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

149. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

150. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class members in an unsafe and insecure manner.

151. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*

152. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

153. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or

affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

154. Defendant violated Section 5 of the FTCA (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

155. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

156. Defendant violated HIPAA (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with industry standards.

157. Defendant's violation of Section 5 of the FTCA and HIPAA (and similar state statutes) constitutes negligence *per se.*

158. Class members are consumers within the class of persons Section 5 of the FTCA and HIPAA (and similar state statutes) were intended to protect.

159. Moreover, the harm that has occurred is the type of harm the FTCA and HIPAA (and similar state statutes) were intended to guard against. Indeed, the FTC has pursued over

fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

160. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

161. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

162. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of their Private Information; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

163. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and

the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

164. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

165. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

166. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class members in an unsafe and insecure manner.

167. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT III
BREACH OF FIDUCIARY DUTY

168. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

169. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became guardian of Plaintiff's and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, (1) to act primarily for Plaintiff and Class members, (2) for the safeguarding of

their Private Information; (3) to timely notify Plaintiff and Class members of a Data Breach's occurrence and disclosure; and (4) to maintain complete and accurate records of what information (and where) Defendant did and does store.

170. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with its customers and/or its clients' plan members, in particular, to keep secure their Private Information.

171. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members because of the high degree of trust and confidence inherent to the nature of the relationship between Plaintiff and Class members on the one hand and Defendant on the other, including with respect to their Private Information.

172. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

173. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class members' Private Information.

174. Defendant breached its fiduciary duties owed to Plaintiff and Class members by failing to timely notify and/or warn Plaintiff and Class members of the Data Breach.

175. Defendant breached its fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff's and Class members' Private Information.

176. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities

remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of their Private Information; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

COUNT IV
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT

177. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

178. Upon information and belief, Defendant entered into a contract(s) to provide secure file transfer services to Plaintiffs and the Class, which services included adequate data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it (i.e., that of Plaintiff and the Class).

179. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class members were the intended direct and express beneficiaries of such contracts.

180. Defendant knew that if it were to breach these contracts, Plaintiff and the Class, would be harmed.

181. Defendant breached its contracts and, as a result, Plaintiff and Class members were

harmed by the Data Breach when Defendant failed to use reasonable data security measures that could have prevented the Data Breach.

182. As foreseen, Plaintiff and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and transfer the files containing their Private Information, including but not limited to, the present and continuous risk of harm through the loss of their Private Information.

183. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT V
UNJUST ENRICHMENT

184. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

185. This claim is pleaded in the alternative to the breach of third-party beneficiary contract claim above.

186. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they paid for products and/or services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class members should have received from Defendant the products and/or services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

187. Defendant knew that Plaintiff and Class members conferred a benefit on it in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving products and/or services from Defendant. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private

Information of Plaintiff and Class members for business purposes.

188. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class members.

189. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

190. Defendant, however, failed to secure Plaintiff's and Class members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class members provided.

191. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiff and Class members and derived revenue by using it for business purposes. Plaintiff and Class members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

192. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

193. If Plaintiff and Class members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

194. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class members' Personal

Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

195. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

196. Plaintiff and Class members have no adequate remedy at law.

197. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of their Private Information; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

198. As a direct and proximate result of Defendant's conduct, Plaintiff and Class

members have suffered and will continue to suffer other forms of injury and/or harm.

199. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid for Defendant's services.

PRAYER FOR RELIEF

Plaintiff, individually, and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against Nuance as follows:

A. Certifying the Class as requested herein, designating Plaintiff as a Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, punitive damages, restitution, and disgorgement;

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

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under

law.

JURY TRIAL DEMANDED

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

Dated: October 3, 2023

Respectfully submitted,

/s/ Randi Kassan

Randi Kassan
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza
Garden City, NY 11530
Telephone: (212) 594-5300
rkassan@milberg.com

Andrew J. Shamis*
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 400
Miami, FL 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com

Jeff Ostrow*
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
ostrow@kolawyers.com

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

**pro hac vice* forthcoming

Attorneys for Plaintiff and the Putative Class

ClassAction.org
