UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

STEPHEN GYSCEK, individually and on behalf of all others similarly situated, Plaintiff, v. NUVANCE HEALTH and HEALTH QUEST SYSTEMS, INC. d/b/a "HEALTH QUEST" Defendants.	)	**Civil Action No.:** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Stephen Gyscek ("Plaintiff" or "Mr. Gyscek"), on behalf of himself individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following, against Defendants Nuvance Health ("Nuvance") and Health Quest Systems, Inc. ("Health Quest," and together with Nuvance, "Defendants"). Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

NATURE OF THE ACTION

1. The Defendants in this action are healthcare providers and, as such, they are entrusted with some of the most sensitive and personal information imaginable. Applicable law and industry standards require Defendants to implement security measures sufficient to protect such information from disclosure to hackers or other unauthorized parties and, in the event of a data breach, to timely notify all affected individuals. Defendants failed to satisfy both of these requirements, and Plaintiff brings this class action to redress the harm caused by Defendant's failures.

2. Defendants operate seven hospitals and provide healthcare in the Hudson Valley region of New York and in Western Connecticut, a region encompassing approximately 1.5 million people. In the course of its business, Defendants collect patient data and maintain databases of sensitive and personal information obtained from their patients, including Plaintiff and the Class (defined below).

3. Defendants failed to store that information in a reasonably secure and adequately protected manner, contravening various laws as well as industry standards and Defendants' own policies. As a result, cybercriminals were able to harvest the personal information of at least 28,910 of Defendants' patients (the "Breach"), including their financial information (*e.g.*, credit card numbers and bank account information), medical information (including provider names, dates of treatment, diagnosis information, and health insurance claims information), personal information (*e.g.*, Social Security numbers and addresses), and/or other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, their "Personal Identifiable Information" or "PII").

4. After discovering the phishing attack that allowed cybercriminals to access the PII of Plaintiff and members of the Class, Defendants failed to timely notify the affected individuals, waiting almost eleven months before issuing the first notifications to Plaintiff and members of the Class, and seven months later issuing a second round of notifications advising that the cybercriminals had accessed more PII than Defendants originally acknowledged.

5. On May 31, 2019, in a message posted to Defendants' website (the "2019 Notice"), Defendants announced that nearly eleven months earlier, in July 2018, they first learned of a phishing incident that allowed one or more cybercriminals to gain access to the emails and

attachments in several employee email accounts.[1] The 2019 Notice disclosed that on January 25, 2019, nearly five months after the initial discovery of the attack, Defendants "identified [breached] email attachments that contained certain health information," and on April 2, 2019, determined that the breached emails and/or attachments contained patient information, including "names, provider names, dates of treatment, treatment and diagnosis information, and health insurance claims information, related to services some patients received at Health Quest Affiliates between January 2018 and June 2018." On or around the date of the 2019 Notice, Defendants mailed notification letters to patients impacted or potentially impacted by the Breach.

6. Defendants offered no explanation for the delay between the initial discovery of the Breach and the subsequent notification to affected patients.

7. Defendants did, however, release a subsequent notice in January 10, 2020 (the "2020 Notice"), revealing that the Breach had impacted more patients and/or revealed more PII than previously acknowledged in the 2019 Notice, including "names in combination with, [*sic*] dates of birth, Social Security numbers, Medicare Health Insurance Claim Numbers (HICNs), driver's license numbers, provider name(s), dates of treatment, treatment and diagnosis information, health insurance plan member and group numbers, health insurance claims information, financial account information with PIN/security code, and payment card information."[2]

---

[1] *Notice of Privacy Incident* (May 31, 2019), *available at* https://patients.healthquest.org/notice-of-privacy-incident-2/ (last visited March 8, 2020).

[2] Health Quest, *Health Quest ("HQ") announced today it is mailing letters to patients whose information may have been impacted by an email phishing incident* (Jan. 10, 2020), *available at* https://www.prnewswire.com/news-releases/health-quest-hq-announced-today-it-is-mailing-letters-to-patients-whose-information-may-have-been-impacted-by-an-email-phishing-incident-300985051.html (last visited March 8, 2020).

8. On or around the date of the 2020 Notice, Defendants sent another round of notification letters to patients impacted or potentially impacted by the Breach. Defendants stated in the 2020 Notice that impacted persons should receive written notice of the Breach by February 15, 2020.

9. As with the 2019 Notice, Defendants again offered no explanation for the delay between the initial discovery of the Breach and the subsequent notification to affected patients—by the date of the 2020 Notice, approximately eighteen months.

10. Defendants have yet to affirmatively notify impacted patients individually regarding which specific data of theirs were stolen.

11. In a letter dated January 3, 2020 and addressed to Plaintiff, Health Quest informed Plaintiff that, as a result of a phishing scheme in which Health Quest's employees disclosed email account credentials to an unauthorized third party, Plaintiff's PII may have been disclosed to the third party. This PII includes name, health insurance information, and clinical information related to treatment received. The letter added that Plaintiff should "regularly review the statements that you receive from your healthcare insurers and providers. If you identify services that you did not receive, please contact the insurer or provider immediately."

12. In late February, Plaintiff attempted to call a phone number listed in the letter if he had any questions because Plaintiff wanted to understand the nature of the breach and see if Defendants would provide credit monitoring of his accounts. Plaintiff called three separate times but was placed on hold for long stretches of time, totaling about an hour. On the fourth try, after a brief hold, Plaintiff finally reached a representative who informed him that it was Health Quest's belief that his payment information had not been exposed but only his name, health insurance information, including his Medicare and Medicare supplement account information. The

representative also said that he was not eligible for any account monitoring service provided by Defendants.

13. The Breach occurred because Defendants failed to take reasonable measures to protect the Personal Identifiable Information it collected and stored. Among other things, Defendants failed to implement data security measures designed to prevent this attack, despite repeated warnings to the healthcare industry about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers. For example, Defendants failed to maintain basic security measures (such as multi-factor authentication to prevent unauthorized persons from accessing customer data), complex data encryption (which prevents data that were accessed or stolen from being readable or otherwise useful), or adequately train its employees in cybersecurity matters (such as how to spot a phishing attack). Defendants failed to disclose to Plaintiff and the members of the Class the material fact that it did not have adequate data security practices to safeguard customers' personal data, and in fact falsely represented that their security measures were sufficient to protect the PII in their possession.

14. Defendants' failure to provide timely and accurate notice of the Breach to Plaintiff and the members of the Class exacerbated the injuries resulting from the Breach. Defendants inexplicably waited eleven months before first notifying Plaintiff and the Class of the Breach, and another seven months to acknowledge the true scope of the Breach. By failing to provide adequate and timely notice, Defendants prevented Plaintiff and Class members from quickly protecting themselves from the dangers posed by the Breach.

15. Defendants' security failures enabled the criminals behind the Breach to steal Personal Identifiable Information from Defendants' computer systems and put Plaintiff and the

Class members at serious and ongoing risk of direct or identity theft. Defendants' acts and omissions have caused ongoing loss to Plaintiff and Class members from the significant time spent attempting to address, mitigate, and monitor the present and future consequences of the Security Breach, including, as appropriate, review of records for fraudulent charges and healthcare services billed for but not received, cancellation and reissuance of payment cards, purchase of credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, implementation and maintenance of credit freezes, and the stress of managing issues resulting from the Breach.

16. The Breach was caused and enabled by Defendants' violation of their obligations under the law and failure to abide by industry standards and their own policies in regard to implementing adequate security measures. Had Defendants implemented adequate security measures, the Breach could have been prevented or mitigated.

17. As a result of Defendants' actions, Plaintiff has been forced to take remedial steps to protect himself from future loss, including by dedicating significant time that he otherwise would not have in making frequent checks of his accounts and credit to ensure that they are not compromised. Indeed, all of the members of the Class are currently at a very high risk of fraud or identity theft and it is reasonable and necessary for them to take prophylactic protective measures, like the purchase of a credit monitoring service, to prevent and mitigate future loss.

18. Defendant's wrongful actions and/or inaction constitute common law negligence, and Plaintiff brings claims of unjust enrichment, bailment, and for violations of New York General Business Law Sections 349 and 899-a.

19. Plaintiff, on behalf of himself, the Class and the respective subclasses, seek (i) actual damages, economic damages, statutory damages, and/or nominal damages, (ii) exemplary damages, (iii) injunctive relief, and (iv) attorneys' fees, litigation expenses and costs.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; and (2) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

21. This Court has personal jurisdiction over Defendants because Defendants do business in and throughout the State of New York, and the wrongful acts alleged in this Complaint were committed in New York, among other venues.

22. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(1) because Defendants maintain their principal place of business in this District and therefore reside in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the members of the Class' claims also occurred in this District.

PARTIES

23. Plaintiff is an individual residing in Staatsburg, New York, who has been a patient at the Heart Center of Poughkeepsie, NY for about 10 years and a patient at Vassar Brothers Hospital for about 40 years. Both are owned and operated by Defendants. Plaintiff's PII was compromised in the Breach described herein. In a letter dated January 3, 2020 and addressed to Plaintiff, Health Quest informed Plaintiff that, as a result of a phishing scheme in which Health Quest's employees disclosed email account credentials to an unauthorized third party, Plaintiff's PII may have been disclosed to the third party. This PII includes name, health insurance information, and clinical information related to treatment received. The letter added that Plaintiff

should "regularly review the statements that you receive from your healthcare insurers and providers. If you identify services that you did not receive, please contact the insurer or provider immediately."

24. Defendant Health Quest Systems, Inc., d/b/a "Health Quest" is a not-for-profit corporation organized and existing under the laws of the State of New York with a principal place of business located at 1351 Route 55, Lagrangeville, New York 12540.

25. Defendant Nuvance Health is a not-for-profit corporation organized and existing under the laws of the State of New York with a principal place of business located at 1351 Route 55, LaGrangeville, New York 12540. Nuvance is the result of an April 2019 merger between Health Quest and Western Connecticut Health Network. As a healthcare provider with seven hospitals in the Hudson Valley and western Connecticut, Nuvance employs about 2,600 doctors and 12,000 staff and generates approximately $2.4 billion in annual revenues.

FACTUAL ALLEGATIONS

26. Each of the preceding paragraphs is incorporated by reference herein.

A. Background

27. Personal Identifiable Information is a valuable commodity. It is sought after by legitimate businesses to help better understand the market and target advertising, and coveted by criminals who use it to commit fraud and theft.

28. The Federal Trade Commission ("FTC") has recognized that consumer data is a new and valuable form of currency. Pamela Jones Harbour, former Commissioner of the FTC, observed that:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information

> may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[3]

Indeed, consumers' personal data supports a $26 billion per year online advertising industry in the United States.[4]

29. Criminals also value PII as a means to commit theft (using, for example, stolen bank account information) or to effectuate identity fraud (with the help of, *e.g.*, a Social Security number, name, and address).

30. The United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report") that identity thieves use identifying data such as Social Security numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[5] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

31. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[6]

---

[3] *Statement of FTC Commissioner Pamela Jones* Harbour (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), *available at* http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited March 9, 2020).

[4] *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy,* WALL STREET JOURNAL (Feb. 28, 2011), *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited March 9, 2020).

[5] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/new.items/d07737.pdf (last visited March 8, 2020).

[6] *Id.* at 2, 9.

32. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/financial fraud.

33. There may be a time lag between when PII is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

34. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner 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 obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name. Identity thieves 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.[8]

35. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "deep web" black market for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have

---

[7] *Id.* at 29 (emphasis added).

[8] *See* Federal Trade Commission, Warning Signs of Identity Theft, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited March 8, 2020).

openly posted stolen credit card numbers, Social Security numbers, and other PII directly on various websites making the information publicly available.

36. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[9]

37. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole. Medical databases are especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value—whereas a stolen Social Security number, on the other hand, only sells for $1."[10] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

38. The danger posed to healthcare providers by cybercriminals has been widely known for years. A 2015 data breach report issued by the credit reporting company Experian repeatedly warns that healthcare providers are susceptible to cybercrime:

> We expect healthcare breaches will increase — both due to potential economic gain and digitization of records. Increased movement to electronic medical records (EMRs), and the introduction of wearable technologies introduced millions of individuals into the healthcare system, and, in return increased, the potential for data breaches. Healthcare organizations face the challenge of securing a significant amount of sensitive information stored on their network,

---

[9] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, (Mar. 3, 2010) https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited March 8, 2020).

[10] *See Study; Few Aware of Medical Identity Theft Risk*, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited March 8, 2020).

> which combined with the value of a medical identity string makes them an attractive target for cybercriminals.[11]

39. Similarly, the New York Times has reported that "[t]he threat of a hacking is particularly acute in the health care and financial services industries, where companies routinely keep the most sensitive personal information about their customers on large databases."[12]

40. The type of data stored by healthcare providers, the type of data stolen in the Breach, is far more valuable to identity thieves than credit card information and other PII stolen from retailers and other businesses that store customer information. While a credit card can be easily cancelled or replaced, a Social Security number cannot. Moreover, "Fraudsters can use this data to create fake IDs to buy medical equipment or drugs, or combine a patient number with a false provider number and file fictional claims with insurers."[13] For this reason, "Medical information can be worth ten times more than credit card numbers on the deep web."[14]

41. Because healthcare providers amass large troves of PII, including highly desirable medical information, they must be vigilant in ensuring that patient data are protected from hackers and other cybercriminals and that outside vendors and businesses are not permitted to access patients' information.

---

[11] Experian, *2015 Second Annual Data Breach Industry Forecast* (2015), *available at* https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf (last visited March 8, 2020).

[12] *See* Reed Abelson & Matthew Goldstein, *Millions of Quest Customers Targeted in Cyberattack*, N.Y. TIMES (Feb. 10, 2015), https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html (last visited March 8, 2020).

[13] Aatif Sulleyman, *NHS Cyber Attack: Why Stolen Medical Information is so Much More Valuable than Financial Data*, INDEPENDENT (Friday May 12, 2017), *available at* https://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html (last visited March 8, 2020).

[14] *Id.*

42. As a corollary to the uses for PII described above, consumers value keeping their PII private. Researchers have shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[15]

43. When consumers were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use—two concerns at issue here—they valued the restriction of improper access to their data at between $11.33 and $16.58 per website, and prohibiting secondary use to between $7.98 and $11.68 per website.[16]

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

B. Defendants Failed to Protect the PII of Plaintiff and the Class from Cybercriminals

45. Defendants offer healthcare services to patients throughout their hospitals, physician practices, and other healthcare providers.

46. These services encompass the storage and maintenance of electronic data containing PII, including that of Plaintiff.

47. On May 31, 2019, Defendants announced an "ongoing investigation of an incident that may have involved some patients' information." The 2019 Notice explained:

---

[15] Hann *et al*., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited March 9, 2020); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011).

[16] *Id.*

> On April 2, 2019, through Health Quest Affiliates' ongoing investigation of a phishing incident, Health Quest Affiliates determined an unauthorized party may have gained access to emails and attachments in several employee email accounts that may have contained patient information. Health Quest Affiliates first learned of a potential incident in July 2018, when several employees were deceived by a phishing scheme, which resulted in certain workforce members being tricked into inadvertently disclosing their email account credentials to an unauthorized party. Although these phishing emails appeared to be legitimate, they were sent by an unknown actor and were designed to have the recipients disclose their email account usernames and passwords. Upon learning of the incident, the employee email accounts in question were secured and a leading cybersecurity firm was engaged to assist us in our investigation. As part of the investigation, Health Quest Affiliates performed a comprehensive review of the contents of the email accounts in question to determine if they contained any sensitive information.
>
> Through this ongoing review, on January 25, 2019, Health Quest Affiliates identified email attachments that contained certain health information, and on April 2, 2019, were determined to contain patient information, which may have included names, provider names, dates of treatment, treatment and diagnosis information, and health insurance claims information, related to services some patients received at Health Quest Affiliates between January 2018 and June 2018.

48. The 2019 Notice also assured patients that "[t]o help prevent a similar incident from occurring in the future, Health Quest Affiliates are implementing multi-factor authentication for email and additional procedures to further expand and strengthen its security processes. Health Quest Affiliates are also providing additional training to its employees regarding phishing emails and other cybersecurity issues."

49. On or around the date of the 2019 Notice, Defendants mailed notification letters to patients impacted or potentially impacted by the Breach—eleven months after the phishing attack occurred, and five months after Defendants first determined that some PII had been exposed. Defendants offered no explanation for this delayed response.

50. According to a May 31, 2019, entry in the breach registry maintained on the Department Health of and Human Services website, the Breach impacted 28,910 individuals.

51. On January 10, 2020, seven months after the 2019 Notice was released, Defendants issued the 2020 Notice, which revealed that the Breach had impacted more patients and/or revealed more PII than previously acknowledged. The 2020 Notice explained:

> On October 25, 2019, through HQ's investigation of a phishing incident, HQ determined some patient information may have been contained in an email account accessed by an unauthorized party. HQ first learned of a potential incident in July 2018, when numerous HQ employees were deceived by a phishing scheme, which resulted in certain HQ employees being tricked into inadvertently disclosing their email account credentials to an unauthorized party. The employee email accounts in question were secured and a leading cybersecurity firm was engaged to assist HQ in its investigation. As part of the investigation, HQ performed a comprehensive review of the voluminous contents of the email accounts in question to determine if they contained any sensitive information. HQ mailed some notification letters in May, 2019. Upon further investigation, HQ determined additional notices were required.
>
> HQ determined emails and attachments in some employees' email accounts contained information pertaining to current and former patients. The information involved varied by individual, but may include names in combination with, dates of birth, Social Security numbers, Medicare Health Insurance Claim Numbers (HICNs), driver's license numbers, provider name(s), dates of treatment, treatment and diagnosis information, health insurance plan member and group numbers, health insurance claims information, financial account information with PIN/security code, and payment card information.

52. Notably, this communication revealed that the Breach was much worse than Defendants had previously acknowledged in the 2019 Notice. The 2020 Notice made clear that the Breach involved several additional types of PII, including financial account and payment card information along with PIN and security codes and Social Security numbers.

53. As in the 2019 Notice, the 2020 Notice stated: "To help prevent something like this from happening in the future, multi-factor authentication for email and additional procedures have been implemented to further expand and strengthen security processes. Additional training to employees regarding phishing emails and other cybersecurity issues has also been offered."

54. On or around the date of the 2020 Notice, Defendants sent another round of notification letters to patients impacted or potentially impacted by the Breach. Defendants stated in the 2020 Notice that persons affected by the Breach should receive notice by February 15, 2020.

55. As discussed in more detail below, Defendants neglected to inform Plaintiff and the Class that Defendants failed to institute appropriate security measures to adequately safeguard their PII. Instead, Defendants represented to Plaintiff and the members of the Class that their PII was safe with Defendants. At all relevant times, Defendants were legally obligated to protect the PII of Plaintiff and the Class and, in the event of a breach of that data, to timely notify Plaintiff and the Class of such a breach. Defendants' failure to institute appropriate protective measures regarding the PII stolen in the Breach is especially egregious because it is well known that PII is a valuable commodity that is coveted by cybercriminals, who regularly attack organizations that possess large collections of such data, and that medical- and health-related data is among the most valuable kinds of PII. Defendants should have known they were likely to be targeted by cybercriminals and should have had appropriate safeguards in place to protect the PII in its possession.

C. Defendants Represented that they were Adequately Safeguarding their Patients' PII

56. Defendants represented that all patient PII they collected, whether in connection with a provider visit or through Defendants' website, would be adequately protected from unlawful disclosure. In various policies, discussed below, Defendants described their obligations regarding

and commitments to patient privacy, detailed the security measures purportedly protecting PII from disclosure, and laid out how and when to notify those affected by a data breach. But Defendants failed to follow their own policies, with respect to both security measures and data breach notification procedures.

57. HIPAA requires Defendants to provide each patient a notice of privacy practices.[17] Defendants' own Notice of Privacy Practices Policy references this obligation, providing that:

> HQ entities must provide the Notice of Privacy Practices (Notice) to all patients and make a good faith effort to obtain a written acknowledgment of receipt of the Notice from each patient, or the patient's Personal Representative, no later than the date of the first service delivery, to the extent practicable. This Notice informs patients how their PHI may be accessed, used and disclosed by HQ, HQ's duty to protect their PHI, and their rights with respect to their PHI and how to exercise those rights.[18]

58. Defendants' Notice of Privacy Practices states that "We are required by law to maintain the privacy of protected health information and to provide individuals with notice of our legal duties and privacy practices with respect to protected health information."[19] It continues:

> OUR PLEDGE REGARDING MEDICAL INFORMATION We understand that medical information about you and your health is personal. We are committed to protecting medical information

---

[17] 45 C.F.R § 164.520.

[18] Health Quest, *Notice of Privacy Practices Policy* (effective February 13, 2019), *available at* https://www.healthquest.org/Uploads/Public/Documents/Compliance/For%20Vendors/Policy%205.2.10-Notice-of-Privacy-Practices.pdf (last visited March 9, 2020); Health Quest, *Notice of Privacy Practices Policy* (effective Feb. 28, 2020), *available at* https://www.healthquest.org/Uploads/Public/Documents/Compliance/Policy%205.2.10%20-%20Notice%20of%20Privacy%20Practices.pdf (last visited March 9, 2020);

[19] Health Quest Medical Practice, P.C., *Notice of Privacy Practices* (effective July 3, 2014), *available at* https://www.healthquest.org/Uploads/Public/Documents/Compliance/English/NOPP-Health-Quest-Medical-Practice.pdf (last visited March 9, 2020). Identical or substantially similar notices for other provider entities within Defendants' network are available here: https://www.healthquest.org/compliance/notice-of-privacy-practices.aspx.

> about you. We create a record of the care and services you receive. We need this record to provide you with quality care and to comply with certain legal requirements. This notice applies to all the records of your care whether made by Entity personnel or your personal doctor . . . where you receive health services.

59. The Notice of Privacy Practices also represents that, in the event of a data breach, "You will be notified [in writing] without unreasonable delay and no later than 60 days after discovery of the breach. Such notification will include information about what happened and what has been done or can be done to mitigate any harm to you as a result of such breach."

60. Defendants made similar representations regarding the safety of information submitted by patients via Defendants' website. Defendants' Website Privacy Policy assures the reader that, "We respect the right to privacy of all visitors to the Health Quest Website," and, except as specifically described in the Website Privacy Policy, "any personal information that you submit is shared only with those people who need this information to respond on behalf of Health Quest to Your question or request" and "unless we have your consent, we will not share any information subject to this Policy outside of our organization for their independent use." The policy further states: "Except as We disclose in this Policy, We do not collect any personally identifiable information about you. If you choose to provide it, We may collect contact personally identifiable information from You, including Your name, email address, home address and phone numbers."

61. Also relevant to the matter at hand is Defendants' Data Protection Policy. That policy "forms the foundations upon which Health Quest manages the confidentiality, availability and integrity of its information and data assets while in transmission and at rest."[20]

---

[20] Health Quest, *Data Protection Policy* (effective December 1, 2015), *available at* https://www.healthquest.org/Uploads/Public/Documents/Compliance/IT/Data%20Protection%20Policy%202016.doc.pdf (last visited March 8, 2020).

62. In relevant part, that policy provides:

> Health Quest management will ensure that [*sic*] following are managed effectively:
>
> • All Health Quest data is classified in accordance with the Security Management policy
> • Data flow analyses which are performed to ascertain where controls are required to protect data according to its classification
> • Data transmission
> • Data storage
> • Encryption and decryption
> • Data backup and recovery
> • Data destruction

63. The Data Protection Policy also classifies data into several categories, including "Sensitive/Confidential," which is defined as:

> Data which is meant to be shared only with those with a business or treatment related need to know. Electronic Protected Health Information as defined by HIPAA and consumer financial information as defined by PCI are both examples of this type of data. But it is not limited to those two definitions. Any data, the exposure of which could cause significant harm to Health Quest or its customers, should be classified as confidential.

64. In regards to data deemed sensitive or confidential, the Data Protection Policy provides that "Health Quest ensures that there are appropriate controls in place to ensure the confidentiality of sensitive data when at rest," *e.g.*, data stored on hard drives or servers. The policy further provides that "[s]ensitive data stored within the Health Quest network are to be encrypted when technically feasible," and "[w]hen [electronic confidential health information] is not stored encrypted, the reason must be documented with compensating controls that are approved by the [Chief Information Security Officer]."

65. Also relevant to the Breach is Defendants' Breach Notification Policy, which "establishes the actions Health Quest Systems, Inc. and its affiliates ("HQ") must take in identifying, managing and responding to potential and confirmed Breaches of patient privacy,

including unsecured protected health information (PHI), in compliance with applicable state and federal laws."[21] This policy provides that "following discovery of a Breach, HQ shall notify each affected individual without unreasonable delay and in no case later than 60 calendar days after the discovery of the Breach. It is the responsibility of HQ to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay."

66. The Breach Notification Policy further clarifies that

> A Breach of unsecured PHI shall be treated as 'discovered' as of the first day such Breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity (includes Breaches by the organization's business associates). The organization is deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or agent (may include certain business associates) of the organization.

67. These notices and policies reveal that Defendants knew the full extent of their obligations to safeguard the PII they collected and stored, and Defendants represented to their patients that PII within their control would be kept safe and subject to appropriate security measures. For example, Defendants "pledged," in their Notice of Privacy Practices, to be "committed to protecting medical information," and stated that the patient would receive timely notice of any data breach involving their PII. These supposed commitments were in fact misrepresentations, as Defendants did not, for example, ensure there were "appropriate controls in

---

[21] Health Quest, *Breach Notification Policy* (effective March 13, 2019), *available at* https://www.healthquest.org/Uploads/Public/Documents/Compliance/For%20Vendors/7-15/Policy-5.2.21--Breach-Notification.pdf (last visited March 8, 2020). This version of the Breach Notification Policy is consistent with an earlier version on Defendants' website dating to February 27, 2014. *See* Health Quest, *Breach Notification Policy* (effective February 27, 2014), *available at* https://www.healthquest.org/Uploads/Public/Documents/Compliance/For%20Vendors/Privacy/Policy%205.2.21%20-%20Breach%20Notification%20for%20Unsecured%20PHI.pdf (last visited March 8, 2020).

place to ensure the confidentiality of sensitive data when at rest"[22] or send notification to Plaintiff and the Class members "no later than 60 days after discovery of the breach."[23]

D. Defendants were Required by Law to Protect the PII of Plaintiff and the Class

68. Defendants also violated duties owed to Plaintiff and members of the Class under federal law, including HIPAA and the Federal Trade Commission Act.

69. HIPAA and implementing regulations require Defendants to establish procedures to keep secure certain PII it possesses, including, without limitation, names and Social Security Numbers. HIPAA requires Defendants to implement reasonable safeguards for such information, which Defendants failed to do.[24]

70. HIPAA regulations also require Defendants to provide notice of any breach resulting in access to unsecured protected health information, *i.e.*, unencrypted health information that unauthorized persons can read or use, to any person whose health information has been or is reasonably believed to be accessed.[25] Under this regulation, Defendants are required to provide notification "without unreasonable delay and in no case later than 60 calendar days after discovery

---

[22] See Health Quest, *Data Protection Policy* (effective December 1, 2015), *available at* https://www.healthquest.org/Uploads/Public/Documents/Compliance/IT/Data%20Protection%20Policy%202016.doc.pdf (last visited March 8, 2020).

[23] Health Quest, *Breach Notification Policy* (effective March 13, 2019), *available at* https://www.healthquest.org/Uploads/Public/Documents/Compliance/For%20Vendors/7-15/Policy-5.2.21--Breach-Notification.pdf (last visited March 8, 2020).

[24] *See* 45 C.F.R. § 164.530(c)(1); 45 C.F.R. § 164.306(a) ("Covered entities and business associates must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information . . . .").

[25] 45 C.F.R. § 164.404.

of a breach."[26] This regulation further provides that a breach is discovered on the first day on which the provider knows of the breach or would have known of the breach "by exercising reasonable diligence."[27]

71. Defendants egregiously failed to provide timely notice of the Breach. The 2019 Notice appeared eleven months after their initial discovery of the phishing attack that led to the Breach—which is on or around the date that they should have known of the Breach—and the 2020 Notice was issued almost seven months later—nearly one and a half years after the initial phishing attack (and in any event more than sixty calendar days after October 25, 2019, the date Defendants claimed to have uncovered the full extent of the Breach). And in both cases members of the Class received their mailed notifications later than the dates of Defendants' notices.

72. Defendants failed to honor their obligations under the law and the duties created by their own policies and promises and representations to Plaintiff and the Class by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting Plaintiff's and the members of the Class' PII;

c. Ensuring the confidentiality and integrity of electronic protected health

d. information they created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

e. Implementing technical policies and procedures for electronic information systems that maintain electronic protected health information to allow

26 *Id.*

27 *Id.*

access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

f. Implementing policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

g. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

h. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. § 164.306(a)(2);

i. Protecting against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3); Ensuring compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Training all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

73. In addition, Defendants had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 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 information.

74. Defendants' data security obligations and promises were particularly important given the substantial increase in data breaches—particularly those impacting the healthcare industry—during the past five years, which were widely known to the public and to anyone in Defendants' industries. Given that Defendants operate in an industry plagued by data breaches and possessed a large trove of valuable data, they were or should have been aware that they were likely targets for cybercriminals.

75. Because of the wealth of information stored on their systems, healthcare providers such as Defendants are or should be aware that they are prime targets for cybercriminals looking for valuable PII.

76. Defendants were or should have been aware of these facts, but failed to institute appropriate safeguards to keep the PII within its possession and control safe from cybercriminals.

E. Plaintiff and the Class Members have been Injured by the Disclosure of their PII

77. Some portion of the monies paid by Plaintiff and the Class to Defendants for medical services was compensation for Defendants' compliance with industry-standard measures with respect to the collection and safeguarding of their PII—or, put another way, the cost of protecting the PII of Plaintiff and the Class was "baked in" to the price Defendants charged for their services. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class overpaid Defendants and thereby incurred actual monetary damages. Plaintiff would have obtained medical services from other suitable providers had Defendants disclosed that they failed to maintain adequate computer systems and

data security practices to safeguard his PII from theft. Plaintiff obtained medical services from Defendant in the past three years.

78. Plaintiff and the Class have suffered additional injury in fact and actual damages including from the substantial lost time in monitoring their accounts and credit history (and in otherwise addressing the Breach) that they have spent as a result of the Breach and that they would not have in its absence. For example, since receiving notification of the Breach, Plaintiff now checks on his banking account with TEG Federal Credit Union – the source of funds to pay for medical services obtained from Defendants – about three or four times a week to make sure everything is in order. Before the Breach, Plaintiff would only check his account on a monthly basis. Plaintiff, as urged by Defendants, also regularly checks his medical documentation to ensure that there are no fraudulent services listed. Plaintiff also spent significant time trying to assess the scope of the breach by reaching out to Defendants after receiving the letter. In late February, Plaintiff attempted to call a phone number listed in the letter if he had any questions because Plaintiff wanted to understand the nature of the breach and see if Defendants would provide credit monitoring of his accounts. Plaintiff called three separate times but was placed on hold for long stretches of time, totaling about an hour. On the fourth try, after a brief hold, Plaintiff finally reached a representative who informed him that it was Health Quest's belief that his payment information had not been exposed but only his name, health insurance information, including his Medicare and Medicare supplement account information. The representative also said that he was not eligible for any account monitoring service provided by Defendants.

79. Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft, the increased risk of identity theft caused by Defendants' wrongful conduct, and the cost of acquiring credit monitoring services.

CLASS ALLEGATIONS

80. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff bring this case as a class action on behalf of a Class defined as follows**:**

> All persons in the United States whose PII was compromised as a result of the Breach

81. The Class is so numerous that joinder of all members is impracticable. The Class has thousands of members. Moreover, the disposition of the claims of the Class in a single action will provide substantial benefits to all parties and the Court.

82. There are numerous questions of law and fact common to Plaintiff and members of the Class. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendants' data security systems prior to the Breach complied with all applicable legal requirements;

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

c. Whether Plaintiff's and other Class members' PII was compromised in the Breach; and

d. Whether Plaintiff's and other Class members are entitled to damages as a result of Defendants' conduct.

83. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Class and have the financial resources to do

84. Plaintiff's claims are typical of the claims of the members of the Class' claims. Plaintiff suffered the same injury as members of the Class—*i.e.*, upon information and belief, Plaintiff's PII was compromised in the Breach.

85. Neither Plaintiff nor their counsel have interests that are contrary to or that conflict with those of the proposed Class.

86. Defendants have engaged in a common course of conduct toward Plaintiff and other members of the Class. The common issues arising from this conduct that affect Plaintiff and members of the Class predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

87. A class action is the superior method for the fair and efficient adjudication of this controversy. members of the Class' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendants. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendants' records and the records available publicly will easily identify the members of the Class. The same common documents and testimony will be used to prove Plaintiff's claims

88. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds that apply generally to members of the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to all members of the Class.

COUNT I
NEGLIGENCE

89. Plaintiff fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

90. Defendants required Plaintiff and members of the Class to submit non-public PII, including names, addresses, credit card information, and Social Security numbers, to obtain medical services, and in the course of Defendants business they generated and stored highly sensitive medical and health-related information pertaining to Plaintiff and members of the Class.

91. Defendants had a duty of care to use reasonable means to secure and safeguard the PII they collected, generated, and stored to prevent disclosure of the information, and to guard the information from theft.

92. Defendants' duty included a responsibility to implement a process by which they could detect a breach of their security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

93. Defendants also owed a duty of care to Plaintiff and members of the Class to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that their systems and networks and the personnel responsible for them adequately protected their customers' PII.

94. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between them and their patients. This duty is recognized by law, including but not limited to HIPAA and the FTCA. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiff and the members of the Class that would arise from a data breach.

95. Defendants' duty to use reasonable security measures also arose under HIPAA, pursuant to which Defendants are required to "reasonably safeguard protected health information

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."[28] The data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

96. In addition, Defendants had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 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.

97. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of confidential PII.

98. Defendants breached their common law, statutory, and other duties by failing to use reasonable measures to protect patients' PII, and by failing to provide timely notice of the Breach.

99. Defendants failed to disclose material information to Plaintiff and the Class at the time they provided their PII, *i.e.*, that Defendants did not have sufficient security or mechanisms to protect PII, and, in fact, represented that they employed adequate security measures.

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

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff' and members of the Class' PII;

[28] C.F.R. § 164.530(c)(1).

b. failing to appropriately train their staff about the dangers of phishing attacks;

c. failing to adequately monitor the security of their network and systems;

d. actively and knowingly misrepresenting or omitting disclosure of material information to Plaintiff and the Class at the time they provided such PII that Defendants did not have sufficient security or mechanisms to protect PII;

e. allowing unauthorized access to Plaintiff's and members of the Class' PII;

f. failing to recognize in a timely manner that Plaintiff's and other members of the Class' PII had been compromised; and

g. failing to warn Plaintiff and other members of the Class about the Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

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

102. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the members of the proposed Class:

a. ongoing, imminent, impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm;

b. actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm;

c. loss of the confidentiality of the stolen confidential data;

d. the illegal sale of the compromised data on the black market;

e. expenses and/or time spent on credit monitoring and identity theft insurance;

f. time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts;

g. decreased credit scores and ratings;

h. lost work time;

i. and other economic and non-economic harm.

103. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seek an order declaring that Defendants' conduct constitutes negligence and awarding damages in an amount to be determined at trial.

COUNT II
UNJUST ENRICHMENT

104. Plaintiff fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

105. Plaintiff and Class members conferred a monetary benefit on Defendants in the form of monies paid for the purchase of health services from Defendants prior to and during the period of the data breach.

106. Defendants appreciates or has knowledge of the benefits conferred directly upon it by Plaintiff and members of the Class.

107. The monies paid for the purchase of health services by Plaintiff and members of the Class to Defendants during the period of the data breach were supposed to be used by Defendants, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and members of the Class.

108. Defendants failed to provide reasonable security, safeguards, and protection for the PII of Plaintiff and Class members and as a result, Plaintiff and Class members overpaid Defendants for the services purchased.

109. Had Plaintiff and the Class known that Defendants would not adequately protect their PII, they would not have elected to purchase health care services from Defendants, or would have paid less for the same services.

110. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and members of the Class, because Plaintiff and Class members paid for adequate safeguards and security measures to protect their PII that Defendant did not provide.

111. Plaintiff and the Class have conferred directly upon Defendants an economic benefit in the nature of monies received and profits resulting from sales and unlawful overcharges to the economic detriment of Plaintiff and the Class members.

112. The economic benefit, including the monies paid and the overcharges and profits derived by Defendants and paid by Plaintiff and members of the Class, is a direct and proximate result of Defendants' unlawful practices as set forth in this Complaint.

113. The financial benefits derived by Defendants rightfully belong to Plaintiff and members of the Class.

114. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiff and the Class.

115. Plaintiff and the Class have no adequate remedy at law.

COUNT III
BAILMENT

116. Plaintiff fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

117. Plaintiff and Class members delivered and entrusted their PHI and PII to Defendants for the sole purpose of receiving services from Defendants.

118. In delivering their PII to Defendants, Plaintiff and Class members intended and understood that Defendants would adequately safeguard their personal and financial information.

119. Defendants accepted possession of Plaintiff and Class members' PHI and PII. By accepting possession, Defendants understood that Plaintiff and Class members expected Defendants to safeguard their personal and financial information adequately. Accordingly, a bailment was established for the mutual benefit of the parties.

120. During the bailment, Defendants owed a duty to Plaintiff and Class members to exercise reasonable care, diligence, and prudence in protecting their PII.

121. Defendants breached their duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' PII, resulting in the unlawful and unauthorized access to and misuse of such information.

122. Defendants further breached their duty to safeguard Plaintiff's and Class members' PII by failing to notify them individually in a timely and accurate manner that their information had been breached and compromised.

123. As a direct and proximate result of Defendants' breach of their duty, Plaintiff and Class members suffered consequential damages that were reasonably foreseeable to Defendants, including but not limited to the damages set forth herein.

COUNT IV
BREACH OF IMPLIED CONTRACT

124. Plaintiff fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

125. When Plaintiff and members of the Class provided their financial, health, and personal information to Defendants in order to purchase services from them, Plaintiff and members of the Class entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to notify Plaintiff and Class members in a timely and accurate manner that their data had been breached and compromised.

126. Plaintiff and Class members would not have provided and entrusted their financial, health, and other PII to Defendants in order to purchase healthcare from Defendants in the absence of the implied contract between them and Defendants.

127. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Defendants.

128. Defendants breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the health, financial, and other PII of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their PII was compromised in and as a result of the Breach.

COUNT V
BREACH OF CONTRACT

129. Plaintiff fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

130. Defendants have a contractual obligation to maintain the security of its customers' personal, health, and financial information, which Defendants recognize in their Notice of Privacy Practices where it addresses the consumers "protected health information."

131. Defendants also specifically promised that they "do not collect any personally identifiable information about you," other than that specifically disclosed in its policy, which did not include dissemination of PII through unsecured email.

132. Defendants breached these contractual obligations by failing to safeguard and protect the PII of Plaintiff and members of the Class, including through the dissemination of PII through unsecured email and through the unauthorized disclosure of PII, including personal, health, and financial information, to unauthorized third parties. Defendants also breached their contractual obligations by failing to provide timely and accurate notice to them that their personal and financial information was compromised in and as a result of the Breach.

133. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of the breaches of the contracts between Defendants and Plaintiff and members of the Class.

COUNT VI
VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349

134. Plaintiff re-alleges and incorporates the preceding paragraphs as if set forth fully herein.

135. New York General Business Law ("GBL") § 349(a) prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce in the furnishing of any service in [New York]" and 349(h) provides for a civil action on behalf of "any person who has been injured by reason of any violation of this section . . . ."

136. As alleged above, Defendants violated the prohibition on deceptive business practices contained in GBL § 349. Defendants' conduct with respect to the PII of Plaintiff and the Class—*i.e.*, the systematic collection and storage of PII without appropriate safeguards— occurred within New York State and is a "business practice" within the meaning of the GBL § 349.

137. Defendants collected and stored the PII of its patients in electronic databases. Defendants knew or should have known that this PII was not protected by reasonable and appropriate security measures that complied with industry standard and all relevant laws and regulations. If Defendants had complied with applicable laws, standards, and norms, they would have prevented the loss or misuse of Plaintiff's and the Class members' PII. Defendants did not disclose to Plaintiff and the Class that they failed to employ appropriate and reasonable measures to protect their PII, and in fact represented that they had sufficient security measures in place.

138. Defendants knew or should have known that their patients were at risk of identity theft and fraud, and yet Defendants, motivated by the desire to maximize profit, failed to apprise Plaintiff and the Class of the danger. Defendants knew or should have known that it could not satisfy its obligations to its patients, both those imposed by law and Defendants' own policies and representations. Defendant's misconduct thus offends public policy and causes substantial injury to consumers.

139. Plaintiff and the Class would not have provided their PII to Defendants if they had known that Defendants failed to employ appropriate and reasonable measures to protect their PII, such as providing adequate employee training regarding phishing and maintaining all PII in encrypted form.

140. Defendants violated GBL §349 by misrepresenting the quality of the security measures employed to protect Plaintiff's and the members of the Class' PII, and Defendants ability to keep Plaintiff's and the members of the Class' PII safe from cybercriminals.

141. Defendants also failed to to timely notify Plaintiff and the Class members of the Breach. Under relevant law and Defendants' own policies, Defendants were required to notify Plaintiff and the Class of the Breach within 60 days of Defendants' discovery (or constructive

discovery) of that event. If Defendants had complied with these requirements, they would have prevented or mitigated the damages of Plaintiff and the Class arising from the Breach.

142. The specific acts and omissions committed by Defendants that violate GBL § 349 include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff' and members of the Class' PII;

b. failing to appropriately train their staff about the dangers of phishing attacks;

c. failing to adequately monitor the security of their network and systems;

d. actively and knowingly misrepresenting or omitting disclosure of material information to Plaintiff and the Class at the time they provided such PII that Defendants did not have sufficient security or mechanisms to protect PII;

e. allowing unauthorized access to Plaintiff's and members of the Class' PII;

f. failing to recognize in a timely manner that Plaintiff's and other members of the Class' PII had been compromised; and

g. failing to warn Plaintiff and other members of the Class about the Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

143. Based on Defendants' representations, among other things, it was reasonably for Plaintiff and the Class to assume that Defendants had employed appropriate safeguards to protect their PII. Defendants did not disclose to Plaintiff and the Class that their PII was in fact vulnerable to cybercriminals. Defendants were the sole possessors of that material information, which they had a duty to disclose.

144. The aforementioned conduct constitutes a deceptive commercial practice in that Defendants have, by the use of false or misleading representations and/or material omissions, misrepresented and/or concealed the fact that (1) their security measures were insufficient and could not adequately protect Plaintiff's and the members of the Class' PII from cybercriminals, and (2) they would or could not notify affected customers of the Breach in a timely manner, as required by law and their own policies.

145. Defendants' misrepresentations and omissions deceived Plaintiff and the Class, who then relied upon those misrepresentations and omissions.

146. The conduct described above would mislead a reasonable consumer and are material, in that a reasonable consumer would be unlikely to entrust their PII with Defendants if they knew that Defendants would and could not protect it.

147. Defendants' wrongful conduct caused Plaintiff and the Class to suffer an injury by causing them to incur substantial expense to protect from misuse of the PII materials by third parties and placing the Plaintiff and the Class at serious risk for monetary damages arising from direct theft and identity fraud. Plaintiff and Class members suffered these damages as a direct and proximate cause of Defendants' conduct.

148. By reason of the foregoing, Defendant's conduct, as alleged herein, constitutes deceptive acts and practices in violation of GBL § 349, and Defendants is liable to Plaintiff and the other members of the Class for the actual damages that they have suffered as a result of Defendant's actions, the amount of such damages to be determined at trial, but not less than $50.00 to each victim of the Breach, treble damages, and/or statutory damages, plus attorneys' fees and costs.

COUNT IV
VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 899-aa

149. Plaintiff fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

150. The acts and practices alleged herein occurred in trade or commerce in the State of New York.

151. The Breach, which compromised the personal information, including the Social Security numbers, of New York citizens constitutes a "breach of security," as that term is defined by NY Gen. Stat.§ 899-aa.

152. In the manner described herein, the defendants unreasonably delayed the disclosure of the breach of security of personal information within the meaning of NY. Gen. Stat. § 899-aa.

153. Pursuant to NY. Gen. Stat. § 89-9aa the Defendants' failure to disclose the breach following the discovery to each New York resident whose personal information was, or was reasonably believed to have been, accessed by an unauthorized person through the breach constitutes an unfair trade practice pursuant to NY. Gen. Stat. § 899-aa.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court enter judgment against Defendants as follows:

A. Certifying this action as a class action, with a Class as defined above;

B. Awarding compensatory damages to redress the harm caused to Plaintiff and members of the Class in the form of, inter alia, direct theft, identity theft, loss of unencumbered use of existing passwords, loss of passwords, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, and other harm. Plaintiff and members of the Class also are entitled to recover statutory damages and/or nominal damages.

Plaintiff and members of the Class' damages were foreseeable by Defendants and exceed the minimum jurisdictional limits of this Court.

C. Ordering injunctive relief including, without limitation, requiring Defendants to (i) provide credit monitoring, (ii) provide identity theft insurance, (iii) institute security protocols in compliance with the appropriate standards and (iv) require Defendants to submit to periodic compliance audits by a third party regarding the security of consumers' personal identifying information its possession, custody and control.

D. Awarding Plaintiff and the Class interest, costs and attorneys' fees; and

E. Awarding Plaintiff and the Class such other and further relief as this Court deems just and proper.

DEMAND FOR TRIAL BY JURY

Pursuant to Federal Rule of Civil Procedure Rule 38, Plaintiff hereby demand a trial by jury.

Dated: April 1, 2020

Respectfully submitted,

MIGLIACCIO & RATHOD LLP

/s/ Nicholas A. Migliaccio
Nicholas A. Migliaccio (New York Bar No. 4035838)
Jason S. Rathod (*pro hac vice* anticipated)
MIGLIACCIO & RATHOD LLP
412 H Street NE, Ste. 302
Washington, DC 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com