UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JOSE APONTE II and LISA ROSENBERG, individually and on behalf of all other persons similarly situated, Plaintiff, vs. NORTHEAST RADIOLOGY, P.C. and ALLIANCE HEALTHCARE SERVICES, INC., Defendants.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Jose Aponte II ("Plaintiff Aponte") and Lisa Rosenberg, ("Plaintiff Rosenberg" (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, complain upon knowledge as to their own acts and upon information and belief as to all other matters against Northeast Radiology, P.C. ("Northeast Radiology") and Alliance HealthCare Services, Inc. ("Alliance HealthCare") (collectively, "Defendants") as follows:

INTRODUCTION

1. This case arises from Defendants' failure to adequately safeguard highly sensitive Electronic Protected Health Information ("e-PHI") collected from Plaintiffs and other Class members. Northeast Radiology is a radiology practice with 4 locations in New York and Connecticut. Alliance HealthCare, a larger national radiology service provider, acquired Northeast Radiology in 2018.

2. Between mid-July 2019 and early September 2019, independent cybersecurity researchers Greenbone Networks ("Greenbone") conducted an analysis of 2,300 medical image archiving systems, also known as Picture Archiving and Communication Systems ("PACS"),

used by radiologists to store medical images.

3. During this investigation, Greenbone uncovered major flaws in Northeast Radiology's and Alliance HealthCare's PACS that permitted unauthorized access to more than 1.2 million patients' medical records. This included at least 61 million x-rays, CT scans, MRIs, and/or other imaging studies that contained extremely sensitive e-PHI, such as medical test results, diagnoses, and procedure descriptions, in addition to patients' names, social security numbers ("SSNs"), dates of birth, and addresses.

4. The Greenbone research team notified Defendants of their findings as early as December 2019, but Defendants ignored them. Instead, Alliance Healthcare and Northeast Radiology continued to leave their PACS exposed, continuing to allow unauthorized third parties to access patient e-PHI.

5. The Greenbone team also notified journalists, including those at TechCrunch, of its findings. TechCrunch published an article on January 10, 2020, detailing the results of Greenbone's investigation. The article specifically identified Defendants and the security flaws in their PACS, including a lack of basic security features, such as encryption or passwords, that permitted unauthorized access to more than 1.2 million patients' records from the Internet.

6. Shortly after the TechCrunch article, a class action was filed in February 2020 against Defendants arising out of their failure to secure their PACS. *See Cohen v. Northeast Radiology, P.C.*, No. 20-cv-01202 (S.D.N.Y.). Significantly, Defendants attempted to discredit the complaint's allegations as based "largely on news accounts" (ECF No. 27-1 at 1) while denying that a breach occurred or that any information was actually accessed by unauthorized third parties. *Id.* at 4.

7. Contrary to these assertions, on March 11, 2020, Northeast Radiology admitted to

the Connecticut Office of the Attorney General that, by at least January 11, 2020, Alliance HealthCare had ***already discovered*** that not only were their PACS exposed, as uncovered by Greenbone, but that "unauthorized individuals" had actually "***accessed*** data from [the] picture archiving and communication system" which stores patients' e-PHI (the "Data Breach" or "breach").

8. Defendants issued a press release that same day (the "March 11 Press Release") confirming the same. The March 11 Press Release was the first time Defendants publicly disclosed "unauthorized individuals gained access to [the] picture archiving and communication system ('PACS')." The March 11 Press Release further revealed that Defendants Northeast Radiology and Alliance HealthCare conducted an internal investigation, which found that at least "29 patients' information was accessed" during the breach. However, Northeast Radiology and Alliance Healthcare admitted that they were unable to determine how many of the "[o]ther patients' information . . . also available on the system" was compromised.

9. The March 11 Press Release also stated that Defendants sent breach notification letters to potentially impacted individuals for whom Northeast Radiology had contact information beginning on March 11, 2020 (the "Breach Notification"). The Breach Notification also disclosed that "unauthorized individuals" had accessed Northeast Radiology's and Alliance HealthCare's PACS data ***for at least nine months*** between April 14, 2019 and January 7, 2020 (the "Breach Period").

10. Defendants also sent the Breach Notification to the New York and Connecticut Attorney General Offices who conducted an investigation into the breach "due to the severity of [the] incident," including because the Data Breach "was not detected for over 9 months" and affected a large number of consumers from each respective state.

11. Such careless handling of e-PHI is prohibited by federal and state law. For example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires healthcare providers, like Defendants, and their business associates to safeguard patient e-PHI through a multifaceted approach that includes, among other things: (a) ensuring the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; (b) proactively identifying and protecting against reasonably anticipated threats to the security or integrity of e-PHI; (c) protecting against reasonably anticipated, impermissible uses or disclosures of e-PHI; (d) putting in place the required administrative, physical and technical safeguards to protect e-PHI; (e) implementing policies and procedures to prevent, detect, contain, and correct security violations; (f) effectively training their workforce regarding the proper handling of e-PHI; and (g) designating individual security and privacy officers to ensure compliance with these policies and procedures.

12. Defendants' failure to comply with HIPAA and other laws and/or guidelines as alleged herein by, among other things, failing to take reasonable steps to safeguard patients' e-PHI, has directly resulted in injury to Plaintiffs and the Class.

13. Plaintiffs and the Class face an ongoing imminent risk of identity theft and fraud because, unlike a credit card, there is no way to cancel e-PHI. The U.S. Department of Health and Human Services ("HHS") has identified several imminent risks as a result of hackers obtaining patients' e-PHI including: (1) medical identity theft, i.e., the use of a patients' medical information to obtain medical services, such as medical prescriptions, surgery, or other medical treatment, as well as counterfeit settlements against health insurers; (2) the weaponization of medical data, i.e., the use of medical data to threaten, extort, or influence the patient to extort money or disparage someone; (3) financial fraud, i.e., the use of e-PHI to create credit card or

bank accounts in the patients' name, taking out loans or lines of credit in the patients' name, or the filing of fraudulent tax documents; and (4) cyber campaigns, using the medical data in combination with other information on the dark web to commit fraud, identity theft, conduct phishing or scams, or obtain the patients' credentials for other services. The "unauthorized individuals" who breached Defendants' systems can continue to exploit this information at the expense of Plaintiffs and the Class. This ongoing imminent risk can often persist for years, as identity thieves often hold stolen data for long periods of time before using it.

14. As Plaintiffs, like other Class members, continue to face an ongoing, imminent risk of fraud and identity theft they will need to, among other things, continuously monitor their financial accounts and/or purchase credit and identity theft monitoring services to alert them of potential misappropriation of their identity to combat the imminent risk of fraud and identity theft.

15. Given the secret nature of, among other things: (a) Defendants' policies, procedures, systems, and controls; (b) the result of the internal investigation into the breach disclosed in the March 11 Press Release; (c) communications among Northeast Radiology and Alliance Healthcare concerning the breach; and (d) vulnerabilities identified by the "leading forensic security firm" referenced in the Breach Notification, Plaintiffs believe that further evidentiary support for their claims will be unearthed after a reasonable opportunity for discovery.

PARTIES

A. Plaintiffs

16. Plaintiff Jose Aponte II is a resident of Fairfield County, Connecticut. Plaintiff Aponte was a patient of Defendant Northeast Radiology and received MRIs at Northeast Radiology in October 2016 and April 2018. At the time of his visit, Plaintiff Aponte provided

Northeast Radiology with e-PHI, including at least his name, address, date of birth, and medical history information. This information, along with other e-PHI associated with Plaintiff's treatment at Northeast Radiology, was stored electronically on Defendants' servers during the Breach Period.

17. Plaintiff Lisa Rosenberg is a resident of Fairfield County, Connecticut. Plaintiff Rosenberg was a patient of Defendant Northeast Radiology and received MRIs at Northeast Radiology in June 2019 and November 2019.

18. At the time of her visit, Plaintiff Rosenberg provided Northeast Radiology with e-PHI, including at least her name, address, date of birth, and medical history information. This information, along with other e-PHI associated with Plaintiff's treatment at Northeast Radiology, was stored electronically on Defendants' servers during the Breach Period.

B. Defendants

19. Defendant Northeast Radiology is a privately held New York Professional Corporation with its principal place of business in Brewster, New York. Founded in 1996, Northeast Radiology offers screening and diagnostic imaging services, including MRIs, CT scans, PET scans, and ultrasounds to patients from four locations in New York and Connecticut.

20. Defendant Alliance HealthCare is a Delaware corporation with its principal place of business in Irvine, California. Alliance HealthCare provides outsourced medical services, *i.e.*, takes over the operation of a practice group within an existing hospital or healthcare system. Currently, it operates radiology, oncology, and interventional medicine practices for more than 1,100 hospitals and other healthcare partners in 46 states.

21. Alliance HealthCare also operates more than 600 radiology systems, ranging from mobile MRI and PET/CT units that are loaded onto trucks to more than 100 fixed-site radiology

installations.

22. In August 2018, Defendant Alliance HealthCare announced a partnership with Northeast Radiology in which Northeast Radiology's New York and Connecticut offices would become part of Alliance HealthCare's radiology division and operate as one of Alliance HealthCare's fixed-site installations.

23. According to the Breach Notification, Alliance HealthCare notified Northeast Radiology that "unauthorized individuals" had accessed Defendants' PACS data for at least nine months during the Breach Period. The information involved in the breach included patients' "name, gender, age, date of birth, exam description and identifier, date of service and medical record number, which may have corresponded to [their] Social Security Number." An internal investigation disclosed in the Breach Notification and the March 11 Press Release identified at least 29 patients whose e-PHI was accessed. However, Defendants were unable to determine the full scope of the breach, including how many of the "[o]ther patients' information . . . also available on the system" was involved.

JURISDICTION AND VENUE

24. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from one Defendant, there are more than 100 Class members, and the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs. For example, Greenbone estimated the value of Plaintiffs' and Class members' data exceeded $1 billion and damages resulting from the "potential risk for medical identity theft" as a result of the exposed PACS to be approximately $3.3 billion. Additionally, given the estimated size of the class (*i.e.*, 1.2 million patients), statutory damages available to Plaintiffs and Class members under New York Gen. Bus. Law § 350 far exceed the $5 million threshold. As does the likely value of any injunctive

relief, including changes to Defendants' systems and procedures, designed to prevent future data breaches.

25. This Court has personal jurisdiction over Defendant Northeast Radiology because it maintains its principal executive offices in Brewster, New York, is registered to conduct business in New York, regularly conducts business in New York, and has sufficient minimum contacts in New York. Defendant Northeast Radiology intentionally avails itself of this jurisdiction by conducting its corporate operations here and promoting, selling, and marketing Northeast Radiology's services to New York consumers and entities.

26. This Court has personal jurisdiction over Alliance HealthCare, as it has sufficient minimum contacts in New York. For example, Alliance HealthCare purposefully availed itself of the privileges and benefits associated with conducting business in this State, by, among other things, reaching into New York to establish a partnership with Defendant Northeast Radiology by which Northeast Radiology's New York offices became part of the Alliance HealthCare radiology group. Thus, Alliance HealthCare regularly conducts business in New York by operating Northeast Radiology as part of its approximately 100 fixed-site radiology systems, in addition to promoting, selling, and marketing Northeast Radiology's services to New York consumers such as Plaintiff.

27. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant Northeast Radiology's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

A. Picture Archiving and Communication Systems and the DICOM Standard

28. In the days before computer technology, when a patient went for medical imaging, including ultrasounds, MRIs, and/or CT scans, the provider would store the results as physical image files in a format similar to an X-ray film. Reviewing those images at a later date required manually accessing those physical files from storage. Sharing images between providers required transporting the physical image files to them for review.

29. Radiologists looking for a more convenient way to store and access medical images developed the PACS in the 1980's. Each PACS consists of four components: (1) an imaging machine (*e.g.*, CT, MRI, or ultrasound), (2) a network for the transmission of images and patient information, (3) workstations for reviewing and interpreting images, and (4) a system where images and reports are stored (referred to as the "PACS server").

30. All PACSs operate according to the Digital Imaging and Communications in Medicine ("DICOM") standard. DICOM was developed by the American College of Radiology and National Electrical Manufacturers Association to create a universal standard for storing, transmitting, and decoding medical images. Prior to the adoption of DICOM, manufactures of imaging machines used proprietary formats for storing digital medical images and networking protocols. This made it difficult for doctors and imaging providers to share medial images because devices manufactured by different vendors used different standards and thus could not communicate with one another.

31. The DICOM standard addressed this issue by creating a new image format (identified by the "dcm" extension) for the storage of medical images and related data. All DICOM-compliant imaging machines, workstations, and servers are required to process and read DICOM files.

32. Also adopted as part of the DICOM standard were specific network requirements regarding not only how imaging files were transmitted but how various DICOM-enabled devices or applications communicate with each other. For example, the DICOM standard requires information transmitted among PACSs to be sent to specific network communication endpoints (called "ports"). So long as the DICOM specific ports are enabled, DICOM files can be exchanged between PACSs or viewed using a DICOM viewer.

B. PACSs and the Internet

33. DICOM has continued to evolve since the 1980's with ongoing changes in technology, like the proliferation of the Internet. For example, as more and more PACSs began to include web-based interfaces to utilize the Internet as their means of communication, DICOM adopted Part 18 of the standard, which sets forth the requirements for making images stored on PACSs accessible over the web.

34. This is especially useful in the radiology field where the radiologist who is taking the image is often not the treating physician. Typically, a treating physician will refer a patient to a radiologist for imaging, but then wants to review the results themselves for diagnostic purposes. And sometimes, after being sent for imaging, a patient may be referred to a hospital or other large healthcare entity for further treatment and the hospital will also want to see the images taken in the radiologist's office. The DICOM protocol allows for all three of these providers to view the patient files. For example, a referring physician that wishes to review a patient's images will download a DICOM viewer application and use the Internet to connect to the radiologist's PACS servers. Once connected, the physician can easily search for, retrieve, and view the DICOM files related to their patient.

35. DICOM guidelines state that in order to protect patient data, PACS servers

should never be kept directly connected to the Internet such that they are accessible without authentication (*e.g.*, a password or encryption key). Rather, PACS servers should be protected behind network security systems that monitor incoming and outgoing network traffic based on a defined set of security rules (*i.e.*, a "firewall") to prevent unauthorized access. Providers that want to offer remote access to images stored on their PACS servers should use a virtual private network ("VPN") that extends their internal PACS network over the public Internet using cryptographically secure methods that require authentication to protect patient data. They should not make DICOM images publicly available.

36. Defendants operate an integrated PACS system that is connected to the public Internet. For example, Northeast Radiology advertises on its website that its PACS servers are available over the Internet to external referring physicians who can "quickly and securely log in to review your study" and directs physicians to call Northeast Radiology for support if they experience any issues accessing patient data remotely.

37. Defendant Northeast Radiology also allows patients to view their test results over the Internet using a DICOM viewer. As advertised on its website, "[p]atients at Northeast Radiology who register for our patient portal, and have compatible software, can access all of their results using our secure HIPAA compliant on-line server at any time from any place after three business days of their exam. Your physician also has on-line access to your results and images using our secure server."

38. However, as explained below, Defendant Northeast Radiology and Alliance HealthCare failed to comply with DICOM guidelines and simply connected their network and servers to the public Internet without utilizing passwords, firewalls, or VPNs to protect patients' data. *See* Part D, below. This allowed unauthorized third parties to access patient data stored on

Northeast Radiology's and/or Alliance HealthCare's PACS servers, resulting in damage to Plaintiffs and the Class. *See* Part J, below.

C. PACSs Contain Highly Sensitive e-PHI

39. Unlike other file types, DICOM files stored on PACS servers allow for additional information to be embedded with the imaging data. For example, a DICOM record will often contain the patient's name, date of birth, date of the examination, scope of the investigation, type of imaging procedure, the attending physician, the institute/clinic, and the number of generated images. Some institutions may also include the patient's SSN as a unique identifier so that the image files can be easily associated with the patient and are not inadvertently lost.

40. As a result, an unauthorized third party that gains access to a PACS acquires a wealth of highly sensitive e-PHI, including not only medical images but the data embedded in those images as part of the DICOM format.

41. Further, PACS systems are often integrated with other systems such as hospital information and electronic medical records systems. These other integrated systems contain even more patient data, including a patient's demographic information such as their full name, SSN, address, employment history, family history, and financial information like credit cards and bank numbers, as well as a patient's past medical history, including doctor visits and previous diagnoses received.

42. This is consistent with the Breach Notification, which disclosed that "unauthorized individuals," once inside Northeast Radiology's and Alliance Healthcare's PACS servers, were able to access e-PHI, including a patient's name, gender, age, date of birth, exam description, and medical record number/SSN.

43. This e-PHI can be used for malicious purposes, including financial fraud, medical identity theft, identity theft, insurance fraud, and crafting convincing phishing messages. HHS has listed a number of scenarios that exploit patient data:

a. *medical identity theft*—the use of another person's medical information to obtain a medical service;

b. *weaponizing of medical data*—the use of sensitive medical data to threaten, extort, or influence individuals;

c. *financial fraud*—the use of personally identifiable information contained in medical records to create credit card or bank profiles to facilitate financial fraud; and

d. *cyber campaigns*—the use of medical data as complementary data in future hacking campaigns.

44. As a result, e-PHI has become increasingly valuable on the black market. For example, according to Forbes, as of April 14, 2017, the going rate for an SSN is $.010 cents and a credit card number is worth $.025 cents, but medical records containing e-PHI could be worth hundreds or even thousands of dollars. For example, in April of 2019, HHS estimated that the average price of medical records containing e-PHI ranged between $250 and $1,000.

45. According to The World Privacy Forum, a nonprofit public interest group, one of the reasons for this price differential is that criminals are able to extract larger illicit profits using medical records than they are for a credit card or SSN. For example, while a credit card or SSN typically yields around $2,000 before being canceled or changed, an individual's e-PHI typically yields $20,000 or more. This is because, in addition to the fact that healthcare data and e-PHI are immutable (*e.g.*, you cannot cancel your medical records), healthcare data breaches often take much longer to be discovered, allowing thieves to leverage e-PHI for an extended period of time.

46. Researchers at HealthITSecurity.com have also reported criminals selling illicit access to compromised healthcare systems on the black market, which would give other

criminals "access to their own post-exploitation activity, such as obtaining and exfiltrating sensitive information, infecting other devices in the compromised network, or using connections and information in the compromised network to exploit trusted relationships between the targeted organizations and other entities to compromise additional networks."

D. Defendants' PACS Servers Are Not Secure

47. Between mid-July 2019 and early September 2019, Greenbone conducted an analysis of approximately 2,300 PACS servers it was able to identify on the Internet.

48. Of these 2,300 PACS servers, 590 allowed for e-PHI to be freely accessed using a publicly available DICOM viewer, *i.e.*, users were not required to enter a password, provide a certificate, or circumvent any other protective measures to access patient data. In 39 instances, e-PHI was transmitted from the PACS servers as unencrypted plain text, making it readable to anyone on the Internet, without the need for a DICOM viewer.

49. As one cybersecurity researcher put it, accessing e-PHI on the 590 unprotected PACS servers Greenbone discovered was "not even hacking. It's walking into an open door." Greenbone confirmed that the process is so simple "everyday internet users could gain access with a few simple actions."

50. One of the PACS servers providing open access to patient data belonged to and/or were operated by Defendants Northeast Radiology and Alliance HealthCare. Greenbone identified Defendants as having the largest cache of unsecured medical data in the U.S. with more than 61 million images from approximately 1.2 million patients' unencrypted records that were accessible without a password through the public internet using publicly available, free tools.

51. Greenbone found that the files stored on the 590 unsecured PACS servers (like those operated by Defendants) contained extremely sensitive e-PHI, including patient names, birthdays, dates of examinations, descriptions of treatment and procedures performed, the identity of attending physicians, name of the institute or clinic, and number of generated images. Greenbone estimates that the value of this data would exceed $1 billion on the "dark web," where criminals buy and sell stolen personal information.

52. Greenbone also estimated that, based on the information contained on Defendants' PACS, that the "potential risk for medical identity theft" alone "sums up to about $3.3 billion."

53. Northeast Radiology confirmed Greenbone's findings in the March 11 Press Release, which stated that "[o]n January 11, 2020, Alliance HealthCare Services notified Northeast Radiology that unauthorized individuals gained access to [the] picture archiving and communication system ('PACS')." The March 11 Press Release further revealed that Defendants Northeast Radiology and Alliance Health Care conducted an internal investigation in light of this information and were able to confirm that at least "29 patients' information was accessed." However, Defendants Northeast Radiology and Alliance Healthcare were unable to confirm how many "other patients' information . . . available on the system" was also compromised.

54. Subsequently, the Attorney Generals of New York and Connecticut opened investigations into the Data Breach given its "severity," Defendants failure to identify the breach for over nine months, and the large number of impacted individuals from New York and Connecticut.

E. Defendants Failed to Comply with HIPAA, the National Standard for Protecting Private Health Information

55. HIPAA requires the healthcare industry to have a generally accepted set of security standards for protecting health information. HIPAA defines Protected Health Information ("PHI") as individually identifiable health information and e-PHI that is transmitted by electronic media or maintained in electronic media. This protected information includes: names, dates, phone numbers, fax numbers, email addresses, SSNs, medical record numbers, health insurance beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, photographs, and any other unique identifying number, characteristic, or code.

56. To this end, HHS promulgated the HIPAA Privacy Rule in 2000 and the HIPAA Security Rule in 2003. The security standards for the protection of e-PHI, known as "the Security Rule," establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' e-PHI.

57. Defendants Northeast Radiology and Alliance HealthCare are either entities covered by HIPAA, *see* 45 C.F.R. § 160.102, or "business associates" covered by HIPAA, *see* 45 C.F.R. § 160.103, and therefore must comply with the HIPAA Privacy Rule and Security Rule, *see* 45 C.F.R. Part 160 and Part 164, Subpart A, C, and E.

58. HIPAA limits the permissible uses of e-PHI and prohibits the unauthorized disclosure of e-PHI. *See* 45 C.F.R. § 164.502. HIPAA also requires that covered entities implement appropriate safeguards to protect this information. *See* 45 C.F.R. § 164.530(c)(1).

59. The electronically stored images and healthcare information accessed by unauthorized third parties on Defendant Northeast Radiology's and/or Alliance HealthCare's PACS servers are e-PHI under the HIPAA Privacy Rule and the Security Rule, which protects all e-PHI a covered entity "creates, receives, maintains or transmits" in electronic form. 45 C.F.R. § 160.103.

60. The Security Rule requires covered entities, including Defendants Northeast Radiology and Alliance HealthCare, to implement and maintain appropriate administrative, technical, and physical safeguards for protecting e-PHI. *See* 45 C.F.R. § 164.530(c)(1). Among other things, the Security Rule requires Northeast Radiology and Alliance HealthCare to identify and "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of [the] information" and "[p]rotect against any reasonably anticipated uses or disclosures." 45 C.F.R. § 164.306.

61. HIPAA also obligates Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations. *See* 45 C.F.R. § 164.308(a)(1)(i).

62. HIPAA further obligates Defendants to ensure that their workforces comply with HIPAA security standard rules, *see* 45 C.F.R. § 164.306(a)(4), to effectively train their workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

63. Defendants failed to comply with these HIPAA rules. Specifically, Northeast Radiology and Alliance HealthCare failed to put in place the necessary technical and non-technical safeguards required to protect Plaintiffs and other Class members' e-PHI and,

moreover, failed to correct those deficiencies after Greenbone notified Defendants that they were able to access e-PHI stored on Defendants' PACS servers from the Internet.

F. Defendants Failed to Timely Notify Plaintiffs and Class Members of the Breach

64. HIPAA requires that Defendants notify each individual whose e-PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of a breach. *See* 45 C.F.R. §§ 164.404(a)(1). Furthermore, Defendants must provide notice "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." *See* 45 C.F.R. § 164.404(b).[1]

65. Greenbone's and other "unauthorized individuals[']" access to e-PHI on Defendants' PACS servers constitute a "breach," which is defined in 45 C.F.R. § 164.402(1) to include the "acquisition, access, use or disclosure of protected health information."[2] As a result, Defendants were required to notify Plaintiffs and Class members within 60 calendar days after discovery of the breach.

66. Defendants did not send notice within 60 calendar days after learning of the breach as required by 45 C.F.R. § 164.404(b). According to TechCrunch, Greenbone notified Defendants that they had accessed e-PHI stored on Defendants' PACS servers without authorization at least one month prior to January 10, 2020. Defendants did not send notice to Plaintiffs or Class members until at least March 11, 2020. This is approximately three months after Greenbone first notified Defendants of the breach.

---

[1] Similar breach notification provisions implemented and enforced by the Federal Trade Commission ("FTC"), apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the Health Information Technology for Economic and Clinical Health Act.

[2] The International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) also defines a data breach as a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.

67. As a result, Defendants' notice did not comply with 45 C.F.R. § 164.404(b). Defendants' failure to provide timely notice as required by the statute significantly increased the risk of harm to Plaintiffs and the Class by depriving them of the ability to take necessary precautions to protect their identities once Defendants learned of the breach.

G. Defendants Failed to Comply with Federal Trade Commission Requirements

68. Defendants Northeast Radiology and Alliance HealthCare were (and still are) prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce" by the Federal Trade Commission Act, 15 U.S.C. § 45. Their failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates this rule.

69. In 2007, the FTC published guidelines establishing reasonable data security practices for businesses. The 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 for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying 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.

70. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

71. Defendants Northeast Radiology and Alliance HealthCare were aware of and failed to follow the FTC guidelines and failed to adequately secure patients' data stored on their PACS servers. For example, the March 11 Press Release explicitly references the FTC and the resources it provides regarding the prevention of identity theft. Furthermore, by failing to have reasonable data security measures in place, Northeast Radiology and Alliance HealthCare engaged in an unfair act or practice within the meaning of § 5 of the FTC Act.

72. In addition to the FTC Act, Defendants had a duty to adopt reasonable data security measures in accordance with the laws of the various states in which it operates, including Conn. Gen. Stat. § 42-471, which require Defendants to safeguard "data, computer files and documents" containing individuals' personal information "from misuse by third parties" and N.Y. Gen. Bus. Law § 899-aa, which require entities to send notice to individuals impacted by a data breach "in the most expedient time possible and without unreasonable delay."

H. Defendants Violated Their Common Law Duty of Reasonable Care

73. In addition to obligations imposed by federal and state law, Defendants owed and continue to owe a common law duty to Plaintiffs and Class members—who entrusted Northeast Radiology and/or Alliance HealthCare with their sensitive e-PHI—to exercise reasonable care in receiving, maintaining, storing, and deleting the e-PHI in Defendants' possession.

74. Defendants owed and continue to owe a duty to prevent Plaintiffs' and Class members' e-PHI from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. An essential part of Defendants' duty was (and is) the obligation to provide reasonable security consistent with current industry best practices and requirements, and to ensure information technology systems and networks, including the PACS servers, in addition to

the personnel responsible for those systems and networks, adequately protected and continue to protect Plaintiffs' and Class members' e-PHI.

75. Defendants owed a duty to Plaintiffs and Class members, who entrusted Defendants with their extremely sensitive e-PHI, to design, maintain, and test the information technology systems, including the PACS servers that housed Plaintiffs' and Class members' e-PHI, to ensure that the e-PHI in Defendants' possession was adequately secured and protected.

76. Defendants owed a duty to Plaintiffs and Class members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the e-PHI stored in Defendants' PACS servers and other computer systems. This duty required Defendants to adequately train employees and others with access to Plaintiffs' and Class members' e-PHI on the procedures and practices necessary to safeguard such sensitive information.

77. Defendants owed a duty to Plaintiffs and Class members to implement processes that would enable Defendants to timely detect a breach of its information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

78. Defendants owed a duty to Plaintiffs and Class members to disclose when and if Defendants' information technology systems, including any PACS servers, and data security practices were not sufficiently adequate to protect and safeguard Plaintiffs' and Class members' e-PHI.

79. Defendants violated these duties. For example, Defendants failed to detect a breach of their PACS servers that had been ongoing *for almost nine months* when Greenbone notified them of the issue. This demonstrates that Defendants did not implement measures designed to timely detect a breach of their information technology systems, as required to

adequately safeguard Plaintiffs' and Class members' e-PHI. Defendants also violated their duty to create, implement, and maintain reasonable data security practices and procedures sufficient to protect Plaintiffs' and Class members' e-PHI. As the Breach Notification states, Alliance HealthCare "retained a leading forensic security firm to assist in its investigation and to evaluate systems and processes to further strengthen protections for the PACS" *after the breach* occurred. Defendants should have taken these steps beforehand to protect the e-PHI in their possession and prevent the breach from occurring, as required under HIPAA, FTC guidelines, and DICOM standards, as well as other state and federal law and/or regulations.

80. Defendants owed a duty to Plaintiffs and Class members to timely disclose the fact that a data breach, resulting in unauthorized access to their e-PHI, had occurred.

I. Defendants Failed Comply with Their Own HIPAA Privacy Policy

81. Northeast Radiology has dedicated a section on its website to apprise its customers, including Plaintiffs and Class members, of the permissible uses and disclosure of their medical records.[3] More specifically, Northeast Radiology posts on its website a Notice of Privacy Practices ("Privacy Practices"), which Defendants Northeast Radiology and Alliance HealthCare admit they are required to comply with ("We [meaning Alliance HealthCare and its affiliates, such as Northeast Radiology] are also required to comply with this Notice of Privacy Practices").

82. At all relevant times, the Privacy Practices defined "Protected Health Information" broadly, as "information about [the patient], including demographic information, that may identify [the patient] and that relates to [the patient's] past, present, or future health care

[3] Northeast Radiology, Notice of Privacy Practices, effective Aug. 23, 2013, available at https://www.nerad.com/hippaa/, (last accessed Feb. 11, 2020).

related services." Accordingly, the definition of Protected Health Information in Defendants' Privacy Practices is consistent with HIPAA, and as such, encompasses PHI and e-PHI, including the personal information Plaintiffs provided to Northeast Radiology, such as their names, addresses, dates of birth, and medical history, all of which fall squarely within the protections provided for by the Privacy Practices.

83. Defendants' Privacy Practices also lists the permitted uses and disclosures of patients' e-PHI and informs patients that e-PHI will be used only "***to support [patients'] care and treatment, to ensure that we will receive payment for charges, and to support our administrative operations***." The Privacy Practices further specify that the e-PHI will only be disclosed if such disclosure is necessary for: (i) treatment, including sharing information with other physicians necessary to diagnose and treat the patient's condition; (ii) payment, including determination of insurance coverage eligibility, verification of patient's insurance benefits, determination of medical necessity, and insurance billing; and (iii) health care operations, including coordination with business partners and suppliers and the making of appointments for patient's medical procedures. Critically, none of the permissible uses of e-PHI include granting unrestrained access to unauthorized third parties who intend to misuse such information for illicit purposes.

84. Defendants' Privacy Practices assure consumers, such as Plaintiffs and Class members, of their "***opportunity to impose limitations on [the] use and disclosure [of personal information]***" in circumstances when the information is not routinely permitted to be disclosed. These include sharing of information with "members of [the patient's] immediate family, other relatives, or [patient's] legally designated health care decision maker." To that effect, the Privacy Practices provide: "***You may prevent this disclosure or you may seek to limit it.*** You may also

designate someone other than those listed above (such as close personal friend) to whom we may disclose your [e-PHI]."

85. The Privacy Practices warned consumers of certain limited situations of compelled disclosures when patients' information may be disclosed without their ability to object to such disclosure—none of which apply to the circumstances here—including: (i) when the disclosure is required by law, and (ii) to demonstrate Defendants' compliance with laws in cases when non-compliance is suspected.

86. For all other situations—*i.e.*, those not covered by routine or compelled disclosure—Defendants' Privacy Practices explicitly promised that any "***use or disclosure of [patient's e-PHI] will occur only with [the patient's] written authorization*** [including] requests [patient] make[s] to Alliance, as well as those [Defendants] may receive from third parties." The Privacy Practices further assuaged patients' concerns regarding unauthorized disclosure of their personal information by allowing them to revoke any written authorizations: "***You may later revoke your authorization, in writing, if you change your mind.***"

87. By these representations in the Privacy Practices, Defendants have affirmatively—and misleadingly—assured patients, including Plaintiffs and the Class members, that they had the ability to control the dissemination of their e-PHI and to restrict its use and access by third parties. The Privacy Practices also expressly guaranteed Defendants would safeguard patients' e-PHI consistent with the applicable laws and regulations. However, Defendants Northeast Radiology and Alliance Healthcare failed to safeguard patients' e-PHI in violation of their own Privacy Practices and applicable law and regulations, as confirmed by the March 11 Press Release, in which Defendants admit that "unauthorized individuals . . . gained access to [the] picture archiving and communication system ('PACS')." In fact, Defendants

failed to take *any* steps to safeguard Plaintiffs' and Class members' e-PHI until long after the Data Breach occurred, and TechCrunch repeatedly followed up on the status of the breach.

88. Defendants' failure to implement appropriate security measures and adequately safeguard Plaintiffs' and Class members' e-PHI violated the terms of their own Privacy Practices.

J. That Data Breach Damages Plaintiffs and Class Members

89. As a result of Defendants' deficient security measures and inability to secure their PACS, Plaintiffs and Class members have been harmed by the compromise of their e-PHI.

90. Plaintiffs and Class members face a substantial and imminent risk of fraud and identity theft. Unlike Greenbone, who accessed Defendants' PACS for purposes of studying the overall security of PACS in general, the other undisclosed and unauthorized individuals who accessed sensitive e-PHI on Defendants' PACS did not have similar academic motives. Several criminal syndicates, including Ukraine's UNC1878 and China's Dynamite Panda, along with various state-sponsored groups, are known to target hospitals and healthcare providers based on the high value associated with e-PHI, both as a revenue stream (*e.g.,* when sold on the dark web, or used to commit identify theft) and as a tool for executing future hacks (*e.g.*, by impersonating users or providing information that can be useful in cracking passwords or security questions). Plaintiffs reasonably anticipate that the identity of the hackers involved in the Data Breach will be revealed in discovery.

91. Plaintiffs' and Class members' substantial and imminent risk of fraud and identity theft is compounded by the fact that e-PHI, including SSNs, are some of the most sensitive forms of data and readily useable to commit fraud by opening accounts in individuals' names or to carry out other financial crimes.

92. Plaintiffs and Class members face an imminent risk of: (1) medical identity theft, such as the use of a patients' medical information to obtain medical services, prescriptions, surgery, or other medical treatment, as well as to obtain counterfeit settlements against health insurers; (2) other forms of identity theft, such as the opening of fraudulent accounts or loans in the individual's name, the use of e-PHI to obtain a driver's license or official identification card in the victim's name but with the thief's picture, the use of the victim's name and SSN to obtain government benefits, and the filing of a fraudulent tax return using the victim's information; and (3) financial fraud, including the unauthorized withdrawal of money from a victim's bank account. Identity thieves may also use e-PHI to obtain a job using the victim's SSN, rent a house, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

93. The Fifth Annual Study on Medical Identity Theft conducted by the Ponemon Institute concluded that medical identity theft alone costs the average victim $13,500 to fix.

94. With respect to the exposed data on Defendants' PACS, Greenbone estimates that "[t]he potential risk for medical identity theft for the affected individuals sums up to about $3.3 billion."

95. Further, identity thieves can combine data stolen in the Data Breach with other information about Plaintiffs and Class members gathered from underground sources, public sources, or even Plaintiffs' and Class members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiffs and Class members to obtain more sensitive information, placing Plaintiffs and Class members at further risk of harm.

96. Because of the imminent risk of fraud and identity theft, Plaintiffs and Class members will be required to spend substantial amounts of time monitoring their accounts for

identity theft and fraud, the opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming. Many Class members will also incur out-of-pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards in the event of fraudulent charges, and similar costs related to the Data Breach.

97. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiffs and Class members must vigilantly monitor their financial accounts *indefinitely*.

98. Defendants acknowledge that Plaintiffs and Class members face a significant risk of various types of identity theft stemming from the Data Breach. Attempting to shift the burden of responding to the Data Breach to consumers, Defendants recommended that affected customers should "remain vigilant about reviewing their account statements and credit reports" and "promptly notify the related financial institution or company and report [fraudulent] activity to the proper law enforcement authorities, including the individuals' local police and their state attorney generals." Thus, Defendants ***acknowledge*** that Plaintiffs and Class members face an actual imminent risk of fraud and identity theft that requires not only immediate action but continuous, ongoing monitoring.

99. Further, while Defendants offered ***some*** customers identity theft monitoring services, Defendants are wholly insufficient to combat the indefinite and undeniable risk of identity theft and fraud, amongst other risks, that may continue long after the Data Breach.

100. Further, Plaintiffs and the Class have sustained additional damages in the form of premiums paid for services that Defendants' represented would include reasonable security measures to protect their e-PHI but that, in reality, did not. Plaintiffs and Class members, at a minimum, are entitled to recover the amount Defendants overcharged them for these less secure services.

CLASS ACTION ALLEGATIONS

101. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and all others similarly situated, as representative of the following class:

> All persons whose e-PHI was maintained on Northeast Radiology's and/or Alliance HealthCare's unsecured PACS server(s) ("the Class").

102. Excluded from the Class are affiliates, predecessors, successors, officers, directors, agents, servants, or employees of Defendants, and the immediate family members of such persons. Also excluded are any trial judge who may preside over this action and their law clerks, court personnel and their family members, and any juror assigned to this action.

103. Plaintiffs reserve the right to amend the Class definition if discovery and/or further investigation reveal that it should be modified.

104. **Numerosity:** The members of the Class are so *numerous* that the joinder of all members of the Class in single action is impractical. For example, Greenbone researchers found more than 61 million images relating to approximately 1.2 million Northeast Radiology and/or Alliance HealthCare patients resided on Defendants' unprotected PACS that were accessed by unauthorized individuals. These Class members are readily identifiable from information embedded within these images and/or from other records in Defendants' possession, custody, or control.

105. **Commonality and Predominance:** There are *common questions of law and fact*

to the Class members, which *predominate* over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendants owed a duty to Plaintiffs and Class members to secure and safeguard their e-PHI;

b. Whether Defendants failed to use reasonable care and reasonable methods to secure and safeguard Plaintiffs' and Class members' e-PHI;

c. Whether Defendants properly implemented security measures as required by HIPAA or any other laws or industry standards to protect Plaintiffs' and Class members' e-PHI from unauthorized access, capture, dissemination and misuse; and

d. Whether Plaintiffs and members of the Class were injured and suffered damages and ascertainable losses as a result of Defendants' actions or failure to act.

106. **Typicality:** Plaintiffs' claims are *typical* of those of other Class members because Plaintiffs' e-PHI, like that of every other Class member, was improperly accessed as a result of Defendants' misconduct, and Plaintiffs and Class members suffered damages as a result.

107. **Adequacy of Representation:** Plaintiffs will fairly and *adequately represent* and protect the interests of the Class. Plaintiffs have retained competent counsel experienced in litigation of complex class actions. Plaintiffs intend to prosecute this action vigorously. Plaintiffs' claims are typical of the claims of all of the other Class members and Plaintiffs have the same non-conflicting interests as the other Class members whose e-PHI was accessed without authorization. Therefore, the interests of the Class members will be fairly and adequately represented by Plaintiffs and their counsel.

108. **Predominance and Superiority:** A class action is *superior* to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of all Class members in a single action

will provide substantial benefits to all parties and to the Court. Damages for any individual Class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendants' violations of law inflicting damages in the aggregate would go un-remedied.

CLAIMS FOR RELIEF

COUNT I
(Negligence)
(Against All Defendants)

109. Plaintiffs incorporate by reference and re-alleges the preceding allegations, as though fully set forth herein.

110. Defendants are providers of radiological services whose patients, including Plaintiffs and Class members, entrust them with highly sensitive e-PHI in connection with these services.

111. Given the highly sensitive nature of e-PHI and likelihood of harm resulting from its unauthorized access, acquisition, use, or disclosure, multiple statutes, regulations, and guidelines, in addition to the common law, impose a duty on Defendants to protect this information. *See, e.g.*, Parts E-H above.

112. For example, the HIPAA Security Rule requires Defendants to: (a) ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; (b) proactively identify and protect against reasonably anticipated threats to the security or integrity of the information; (c) protect against reasonably anticipated, impermissible uses or disclosures; (d) put in place the required administrative, physical and technical safeguards; (e) implement policies and procedures to prevent, detect, contain, and correct security violations; (f)

effectively train their workforce regarding the proper handling of e-PHI; and (g) designate individual security and privacy officers to ensure compliance.

113. Defendants also had a duty to use reasonable data security measures under several state and federal laws, including § 5 of the FTC Act, 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 consumer data.

114. Accordingly, Defendants Northeast Radiology and Alliance HealthCare owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their e-PHI by, among other things: (a) maintaining adequate security systems to ensure that Plaintiffs' and Class members' e-PHI was adequately secured and protected; (b) implementing processes that would detect a breach of Defendants' systems in a timely manner; and (c) timely notifying patients, including Plaintiffs and Class members, that their e-PHI had been accessed, acquired, used, or disclosed as a result of a data breach so that Plaintiffs and Class members could protect themselves from identify theft by transferring their records to a different provider who maintained adequate security controls, obtaining credit and/or identify theft monitoring protection, canceling or changing their bank account and/or debit or credit card information, and/or taking other appropriate precautions.

115. Northeast Radiology and Alliance HealthCare breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' e-PHI by failing to adopt, implement, and maintain adequate security measures. For example, Defendants failed to implement appropriate systems to detect a breach of their PACS servers, as demonstrated by their failure to identify the breach alleged herein, which had been ongoing for *almost nine months*, when they were contacted by Greenbone researchers. Greenbone's and other

"unauthorized individual['s]" ability to access e-PHI stored on Defendants' PACS severs confirms that Northeast Radiology and Alliance HealthCare negligently failed to abide by the HIPAA Security Rule, among other guidelines and regulations, by failing to protect against anticipated threats to the security or integrity of Plaintiffs' and Class members' e-PHI, and any reasonably anticipated impermissible uses or disclosures of their e-PHI.

116. The egregiousness of Defendant's breach of their duty to exercise reasonable care is compounded by the fact that they stored e-PHI on their PACS servers with no security whatsoever. The PACS server was unencrypted and could be accessed from the public Internet and viewed without a password or other credentials.

117. Defendants Northeast Radiology and Alliance HealthCare also breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' e-PHI by failing to timely notify Plaintiffs and Class members that their e-PHI had been accessed by unauthorized third parties. For example, Defendants waited more than 60 days from the time Greenbone researchers informed them of the breach to publicly disclose the breach and notify impacted individuals in violation of 45 C.F.R. § 164.404(b).

118. Defendants' failure to comply with industry regulations such as HIPAA further evidence their negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' e-PHI.

119. It was foreseeable to Defendants that a failure to use reasonable measures to protect its customers' e-PHI could result in injury to its patients. Actual and attempted breaches of data security were reasonably foreseeable to Defendants given the known frequency of data breaches and various warnings from industry experts.

120. The injuries and harm suffered by Plaintiffs and Class members as a result of

having their e-PHI accessed, acquired, used, or disclosed without authorization was the reasonably foreseeable result of Northeast Radiology's and Alliance HealthCare's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' e-PHI. Defendants knew or should have known that the systems and technologies used for storing Plaintiffs' and Class members' e-PHI allowed that information to be accessed, acquired, used, or disclosed by unauthorized third parties. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and Class members, the injuries alleged herein would not have occurred.

121. In connection with the conduct described above, Defendants acted wantonly, recklessly, and with complete disregard for the consequences Plaintiffs and Class members would suffer if their e-PHI was accessed by unauthorized third parties.

122. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members sustained damages as alleged herein. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

123. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class members.

COUNT II
(Negligence *Per Se*)
(Against All Defendants)

124. Plaintiffs incorporate by reference and re-alleges the preceding allegations, as though fully set forth herein.

125. In addition to Defendants' common law duty to exercise reasonable care in securing Plaintiff and Class members' data, several statutes imposed a duty on Defendants to

safeguard highly sensitive e-PHI. Defendants' violation of these statutory duties, as describe below, independently establishes their negligence *per se*.

Negligence *Per Se* Pursuant to HIPAA

126. As alleged above, the HIPAA Security Rule requires Defendants Northeast Radiology and Alliance HealthCare to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI, which Defendants negligently failed to implement.

127. The HIPAA Security Rule also requires Defendants to protect against reasonably anticipated threats to the security or integrity of e-PHI and protect against reasonably anticipated impermissible uses or disclosures, which Defendants negligently failed to do. *See* 45 C.F.R. Part 160 and Part 164, Subpart A and C.

128. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendants to timely notify Plaintiffs and Class members of the breach alleged herein as required by the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414. Defendants did not provide notice until approximately three months after Greenbone first notified Defendants of the breach.

129. Defendants failure to secure Plaintiffs' and Class members' e-PHI and to notify them that such information had been accessed by unauthorized third parties violated at least the following HIPAA regulations:

A) The HIPAA Privacy and Security Rule 45 C.F.R. § 160 and 45 C.F.R. § 164, Subpart A, C, and E

- 45 C.F.R. § 164.306
- 45 C.F.R. § 164.308
- 45 C.F.R. § 164.312
- 45 C.F.R. § 164.314

- 45 C.F.R. § 164.502
- 45 C.F.R. § 164.530

B) The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414

- 45 C.F.R. § 164.404

130. Plaintiffs and Class members are within the class of persons that the HIPAA Privacy and Security Rule were intended to protect, because the HIPAA Privacy and Security rule were expressly designed to protect sensitive patient information.

131. The harm that has occurred is the type of harm that HIPAA was intended to guard against, namely, the disclosure of patients' sensitive patient information, including e-PHI.

132. Likewise, Plaintiffs and Class member are within the class of persons the HIPAA Breach Notification Rule is designed to protect, namely, patients who e-PHI is accessed, acquired, used, or disclosed.

133. The harm that occurred is the type of harm that the HIPAA Breach Notification Rule is intended to guard against, namely, delay in notifying patients whose e-PHI is compromised.

134. Defendants' violations of HIPAA constitute negligence *per se*.

Negligence *Per Se* Pursuant to the FTC Act

135. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendants failure to use reasonable measures to protect e-PHI.

136. Northeast Radiology and Alliance HealthCare violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class members' e-PHI and not complying with industry standards. Defendants' conduct was particularly egregious given the

nature and amount of e-PHI it obtained and stored and the foreseeable consequences of a data breach in a database with more than 61 million images associated with 1.2 million patients across its four offices. The egregiousness of Defendants' conduct is compounded by the fact that their PACS were left completely unsecured, accessible without any password or complex tools, by anyone with an internet connection.

137. Plaintiffs and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect because they paid Defendants for radiological and/or medical goods and services. The harm that has occurred is the type of harm the FTC Act was intended to guard against, namely harm to consumers as a result of unfair practices in commerce.

138. Defendants' violation of Section 5 of the FTC constitutes negligence *per se*.

Negligence *Per Se* Pursuant to Conn. Gen. Stat. § 42-471

139. Pursuant to Conn. Gen. Stat. § 42-471, Defendants had a duty to safeguard "data, computer files and documents" containing individuals' personal information "from misuse by third parties." Conn. Gen. Stat. § 42-471(a).

140. "Personal Information" is defined to include "information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number." Conn. Gen. Stat. § 42-471(b).

141. Defendants breached this duty by failing to use reasonable measures to protect Plaintiffs' and Class members' e-PHI and not complying with industry standards. Defendants' conduct was particularly egregious given the nature and amount of e-PHI it obtained and stored and the foreseeable consequences of a data breach in a database with more than 61 million images associated with 1.2 million patients across its four offices. The egregiousness of Defendants' conduct is compounded by the fact that their PACS were left completely unsecured,

accessible without any password or complex tools, by anyone with an internet connection.

142. Plaintiffs and Class members within the class of persons Conn. Gen. Stat. § 42-471 is designed to protect because its expressly designed to protect individual's personal information.

143. The harm that has occurred is the type of harm Conn. Gen. Stat. § 42-471 was intended to guard against, namely, harm as a result of a person or entity's failure to safeguard individual's personal information.

144. Defendants' violation of Conn. Gen. Stat. § 42-471 constitutes negligence *per se*.

Negligence *Per Se* Pursuant to N.Y. Gen. Bus. Law § 899-aa

145. Pursuant to N.Y. Gen. Bus. Law § 899-aa *et seq.*, Defendants had a duty to send notification to affected New York residents "in the most expedient time possible and without unreasonable delay." N.Y. Gen. Bus. Law § 899-aa(2).

146. N.Y. Gen. Bus. Law § 899-aa(2) provides that "[a]ny person or business which owns or licenses computerized data which includes *private information* shall disclose any *breach of the security of the system* following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay . . . ." (emphasis added).

147. Under N.Y. Gen. Bus. Law § 899-aa(1)(c), "[b]reach of the security of the system" "shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business."

148. Under N.Y. Gen. Bus. Law § 899-aa(1)(a) "Personal information" is defined to mean "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person."

149. Under N.Y. Gen. Bus. Law § 899-aa(1)(b), "Private information" "is defined to include "personal information . . . in combination with . . . [a] social security number" when either the personal information or social security number is not encrypted.

150. Defendants violated N.Y. Gen. Bus. Law § 899-aa(5)(d)(1) since a "clear and conspicuous notice" was not sent to Plaintiffs and Class members "in the most expedient time possible and without unreasonable delay," because Defendants knew that Plaintiffs' and Class members' sensitive data had been accessed by unauthorized individuals for ***several months*** but failed to take any action to notify impacted individuals. Defendants did not publicly disclose or send "clear and conspicuous notice" until at least March 11, 2020, nearly three months after Greenbone first notified Defendants of the Data Breach.

151. Plaintiffs and Class members are within the class of persons N.Y. Gen. Bus. Law § 899-aa is designed to protect because the statute is specifically designed to protect individuals by providing prompt notice when their personal information is compromised

152. The harm that occurred is the type of harm that N.Y. Gen. Bus. Law § 899-aa is intended to guard against, namely, harm caused by delay in notifying individuals whose personal information is compromised.

153. Defendants' violation of N.Y. Gen. Bus. Law § 899-aa constitutes negligence *per se*.

154. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class members have been injured as described herein, and are entitled to damages, including

compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
(Breach of Contract)
(Against All Defendants)

155. Plaintiffs incorporate by reference and re-alleges the preceding allegations, as though fully set forth herein.

156. Defendants expressly promised to safeguard Plaintiffs' and Class members' e-PHI in accordance with the applicable state and federal laws and/or regulations. Specifically, Northeast Radiology and Alliance HealthCare promised to abide by their HIPAA privacy policy, which they provided to patients and customers. *See* ¶¶ 81-88.

157. Defendants also marketed their safety and security as one of the reasons why patients should use them for radiological services. For example, Northeast Radiology's website advertises that it uses "state of the art equipment operated by experienced technologists" and provides a "safe, comfortable, and private full-service imaging centers." Additionally, Northeast Radiology proudly advertises on its website that it has been awarded "the high distinction of being a Diagnostic Imaging Center of Excellence" by the American College of Radiology.

158. This HIPAA privacy policy and representations made in the advertisements cited above applied to Plaintiffs and Class members who entered into a contract with Defendants when they provided their e-PHI to Northeast Radiology and/or Alliance HealthCare as part of a transaction in which they paid money for radiological and/or medical goods and services.

159. Plaintiffs and Class members fully performed their obligations under their contracts with Defendants, including by paying for the radiological and/or medical goods and service Defendants provided.

160. Defendants did not hold up their end of the bargain. In entering into such

contracts, Defendants agreed to protect Plaintiffs' and Class members' e-PHI and provide timely notice if their e-PHI was accessed, acquired, used, of disclosed in accordance with state and federal law and/or regulations, their HIPAA privacy policy, and industry standards.

161. Defendants failed on both accounts: they failed to take reasonable steps to protect Plaintiffs' and Class members' e-PHI and failed to notify Plaintiffs and Class members within 60 days of discovering that their e-PHI was accessed, acquired, used, of disclosed in accordance with 45 C.F.R. § 164.404(b). *See* ¶¶ 59-61, above. Each of these acts constituted a separate breach of the contracts Defendants entered with Plaintiffs and Class members.

162. Plaintiffs and Class members would not have entrusted Defendants with their e-PHI in the absence of the contract between them and Defendants, obligating Defendants to keep this information secure and provide timely notice in the event of a breach.

163. As a direct and proximate result of Defendants' breaches of their contracts, Plaintiff and Class members sustained damages as alleged herein, including when they paid for services that did not include reasonable security measures sufficient to protect Plaintiffs' and Class members' e-PHI, despite Defendants promise that it would do so. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT IV
(Breach of Implied Contract)
(Against All Defendants)

164. Plaintiffs incorporate by reference and re-alleges the preceding allegations, as though fully set forth herein.

165. When Plaintiffs and Class members paid money and provided their e-PHI to Northeast Radiology and Alliance Healthcare in exchange for their services, they entered into

implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect their e-PHI and to timely notify them if their e-PHI had been accessed, acquired, used, or disclosed.

166. Northeast Radiology and Alliance Healthcare solicited and invited prospective customers such as Plaintiffs and Class members to provide their e-PHI as part of its regular business practices. Plaintiffs and Class members accepted Defendants' offers and provided their e-PHI to Defendants.

167. In entering into such implied contracts, Plaintiffs and Class members reasonably believed that Defendants would safeguard and protect their e-PHI and that Defendants would use part of the funds received from Plaintiffs and Class members to pay for adequate and reasonable data security practices.

168. Plaintiffs and Class members would not have entrusted their e-PHI to Defendants in the absence of the implied contract between them and Defendants to keep patients' e-PHI secure.

169. Plaintiffs and Class members fully performed their obligations under the implied contracts with Northeast Radiology and Alliance Healthcare by paying for services.

170. Northeast Radiology and Alliance Healthcare breached their implied contract with Plaintiffs and Class members by failing to safeguard and protect their e-PHI and by failing to provide timely and accurate notice that their e-PHI was compromised as a result of the data breach.

171. Northeast Radiology's and Alliance Healthcare's failure to satisfy its obligations under the implied contracts directly caused the successful intrusion of Defendants' PACS servers and access to Plaintiffs' and Class members' e-PHI.

172. As a direct and proximate result of Defendants' breaches of their implied contracts, Plaintiff and Class members sustained damages as alleged herein, including when they paid for services that did not include reasonable security measures sufficient to protect Plaintiffs' and Class members' e-PHI, despite Defendants promise that it would do so. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT V
(For Violation of New York's Uniform Deceptive Trade Practices Act)
(Gen. Bus. Law § 349 *et seq.*)
(Against All Defendants)

173. Plaintiffs incorporate by reference and re-alleges the preceding allegations, as though fully set forth herein.

174. New York's Uniform Deceptive Trade Practice Act ("GBL § 349") prohibits "deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state." GBL § 349(a).

175. As a large health care facility with locations in New York, Defendants conducted business, trade or commerce in New York State.

176. As a consumer of Northeast Radiology's and Alliance HealthCare's services, Plaintiffs are "person[s]" within the meaning of GBL § 349.

177. Plaintiffs are authorized to bring a private action under New York's Uniform Deceptive Trade Practices Act, Gen. Bus. Law § 349(h).

178. Plaintiffs and Class members provided their e-PHI to Northeast Radiology pursuant to transactions in "business" "trade" or "commerce" as meant by GBL § 349.

179. This Count is brought for Defendants' deceptive conduct, including their unlawful and deceptive acts related to the breach alleged herein.

180. Defendants engaged in unlawful and deceptive acts and practices in the conduct of trade or commerce and furnishing of services purchased by Plaintiffs and the Class in violation of GBL § 349, including but not limited to the following:

a. Defendants failed to implement adequate privacy and security measures to protect Plaintiffs' and Class members' e-PHI from being accessed, acquired, used, or disclosed by unauthorized third parties, which was a direct and proximate cause of Plaintiffs' and Class members' harm;

b. Defendants' representation that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Class members' e-PHI from being accessed, acquired, used, or disclosed by unauthorized third parties was unfair and deceptive given the inadequacy of its privacy and security protections;

c. Defendants omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for Plaintiffs' and Class members' e-PHI;

d. Defendants omitted, suppressed, and concealed material fact, in furnishing medical treatment, by misrepresenting they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Class members' e-PHI;

e. Defendants' negligence in failing to disclose the material fact of its inadequate privacy and security protections for Plaintiffs and Class members e-PHI was deceptive in light of representations that they would comply with, among other things, HIPAA;

f. Defendants engaged in deceptive, unfair, and unlawful acts or practices by failing to take proper action following the Data Breach to enact privacy and security measures and protect Plaintiffs' and Class members e-PHI, including through its failure to even begin to investigate the breach until at least one month after being notified;

g. Defendants engaged in deceptive, unfair, and unlawful acts by publicly denying the Data Breach for several months when, in fact, they knew their PACS had been compromised by unauthorized individuals.

h. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiffs' and Class members' e-PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in Plaintiffs' and the Class' e-PHI being accessed, acquired, used, or disclosed by unauthorized third parties. These unfair acts and

practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and HIPAA; and

i. Defendants held themselves out as using "state of the art equipment operated by experienced technologists" that provides a "safe, comfortable, and private full-service imaging centers," while it knew that its security standards were inadequate.

181. Defendants systematically engaged in these deceptive, misleading, and unlawful acts and practices to the detriment of Plaintiffs and Class members.

182. Defendants willfully engaged in such acts and practices and knew or acted in reckless disregard for whether they violated GBL § 349.

183. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' sensitive customer data.

184. Plaintiffs and Class members relied on Defendants' deceptive acts and practices when they paid money in exchange for goods and services and provided their e-PHI to Northeast Radiology for medical treatment.

185. Plaintiffs and Class members relied on Defendants to safeguard and protect their e-PHI and to timely and accurately notify them if their data had been accessed by unauthorized third parties.

186. Plaintiffs and Class members had no way of knowing Defendants' data security was severely deficient, as only Defendants had exclusive knowledge of its data security practices.

187. The above unfair and deceptive acts and practices by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to

consumers or to competition.

188. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50, whichever is greater, treble damages, injunctive relief, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully requests that the Court:

a. Certify the Class pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class members;

b. Designate Plaintiffs as representatives of the Class and the undersigned counsel, LOWEY DANNENBERG, P.C. as Class Counsel;

c. Award Plaintiffs and the Class actual damages, compensatory damages, and statutory damages in an amount to be determined by the Court and treble and punitive damages to punish Defendants' egregious conduct as described herein, and to deter Defendants and others from engaging in similar conduct;

d. Award Plaintiffs and the Class injunctive relief, as permitted by law or equity, including enjoining Defendants from continuing the unlawful practices set forth herein, ordering Defendants to fully disclose the extent and nature of the security breach and theft, and ordering Defendants to pay for identity theft and credit monitoring services for Plaintiffs and the Class;

e. Award Plaintiffs and the Class statutory interest and penalties;

f. Award Plaintiffs and the Class their costs, prejudgment and post judgment interest, and attorneys' fees; and

g. Grant such other relief that the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury as to all issues stated herein, and all issues so triable.

Dated: July 8, 2021
White Plains, New York

Respectfully submitted,

LOWEY DANNENBERG P.C.

/s/ Christian Levis
Christian Levis
Amanda Fiorilla
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035
Email: clevis@lowey.com
afiorilla@lowey.com

Steven L. Bloch
Ian W. Sloss
SILVER GOLUB & TEITELL LLP
184 Atlantic Street
Stamford, CT 06901
Tel.: (203) 325-4491
Fax: (203) 325-3769
sbloch@sgtlaw.com
isloss@sgtlaw.com

Attorneys for Plaintiffs and the Proposed Class

ClassAction.org