IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

ARIANN J-HANNA and NICOLE PYLE, individually and on behalf of all others similarly situated,	)	Case No.:
Plaintiffs,	)	**CLASS ACTION**
v.	)	
US RADIOLOGY SPECIALISTS, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Ariann J-Hanna ("Plaintiff J-Hanna") and Nicole Pyle ("Plaintiff Pyle") (collectively "Plaintiffs"), individually and on behalf of all others similarly situated, through their undersigned counsel, hereby allege the following against Defendant US Radiology Specialists, Inc. ("US Radiology" or "Defendant"). Facts pertaining to Plaintiffs and their personal experiences and circumstances are alleged based upon personal knowledge, and all other facts herein are alleged based upon information and belief, *inter alia*, the investigation of Plaintiffs' counsel.

NATURE OF THE ACTION

1. This is a class action for damages against US Radiology for its failure to exercise reasonable care in securing and safeguarding sensitive patient data—including first and last names, Social Security numbers, drivers' license information, dates of birth, health insurance information, personal addresses, and medical treatment information (collectively defined herein as "PII" or "Private Information").

2. Plaintiffs bring this action on behalf of similarly situated patients whose sensitive Private Information was stolen by cybercriminals in a cyber-attack on US Radiology's systems

that took place in or around December of 2021 and which resulted in the access and exfiltration of sensitive patient Private Information (the "Data Breach").

3. US Radiology Specialists' subsidiaries, including Radiology Ltd., sent a notice of the Data Breach to Plaintiffs and members of the putative "Class" (defined below).

4. Plaintiffs and Class members were not notified of the data breach until September 2022 – nearly nine months after their Private Information was first accessed and exfiltrated.

5. As a result of the Data Breach and Defendant's failure to promptly notify Plaintiffs and Class members thereof, Plaintiffs and Class members are at imminent and substantial risk of experiencing various types of misuse of their Private Information in the coming years, including but not limited to, unauthorized credit card charges, unauthorized access to email accounts, identity theft.

6. There has been no assurance offered by US Radiology or its subsidiaries that all personal data or copies of data have been recovered or destroyed.

7. Accordingly, Plaintiffs assert claims for negligence, breach of third-party beneficiary contract, breach of implied contract, breach of fiduciary duty, and declaratory and injunctive relief.

PARTIES

A. Plaintiff Ariann J-Hanna

8. Plaintiff Ariann J-Hanna is a resident and citizen of Tucson, Arizona and brings this action in her individual capacity and on behalf of all others similarly situated. J-Hanna has been a patient at Banner Health University Medical Center in Tucson, Arizona, and received medical imagining services from Radiology Ltd., one of US Radiology's subsidiaries. To receive

services from Radiology Ltd., Plaintiff was required to disclose her PII, which was then entered into US Radiology Specialists' database and maintained by Defendant.

9. In maintaining her Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff's PII. Defendant, however, did not implement proper, industry-standard safeguards to protect Plaintiff's PII, leading to its exposure and exfiltration by cybercriminals, which cybercriminals stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

10. In September of 2022, Plaintiff J-Hanna received a notification letter from Defendant's subsidiary stating that her Private Information was compromised by cybercriminals.

11. Unlike most data breach notification letters, the letters Plaintiffs and Class members received did not include any offer of credit monitoring or identity theft protection services.

12. Plaintiff J-Hanna and Class members have faced and will continue to face a certainly impending and substantial risk of future harms because of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, targeted advertising without patient consent, and fraudulent applications for benefits in their names, leading to Class members being denied necessary loans or benefits in the future.

13. Plaintiff J-Hanna greatly values her privacy, especially while receiving medical services, and would not have paid the amount that she did to receive medical services had she known that US Radiology would negligently maintain her Private Information as it did.

B. Plaintiff Nicole Pyle

14. Plaintiff Nicole Pyle is a resident and citizen of Tucson, Arizona and brings this action in her individual capacity and on behalf of all others similarly situated. Pyle has been a

patient at Carondelet Imaging Center in Tucson, Arizona, and received medical imagining services from Radiology Ltd., one of US Radiology's subsidiaries. To receive services from Radiology Ltd., Plaintiff was required to disclose her PII, which was then entered into US Radiology Specialists' database and maintained by Defendant.

15. In maintaining her Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff's PII. Defendant, however, did not implement proper, industry-standard safeguards to protect Plaintiff's PII, leading to its exposure and exfiltration by cybercriminals, which cybercriminals stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

16. In September of 2022, Plaintiff Pyle received a notification letter from Defendant's subsidiary stating that her Private Information was compromised by cybercriminals.

17. Plaintiff Pyle and Class members have faced and will continue to face a certainly impending and substantial risk of future harms because of Defendant's ineffective data security measures, as further set forth herein.

18. In fact, Plaintiff Pyle has already suffered harm due to Defendant's ineffective data security – she has been charged for medical services she never received, causing mental distress and financial problems. This fraudulent misuse of her Private Information has also impacted Plaintiff Pyle's credit score, and she has been forced to delay a house purchase.

C. Defendant US Radiology Specialists

19. US Radiology is a healthcare conglomerate and holding company incorporated in Delaware.

20. US Radiology has a principal place of business at 4200 Six Forks Road, Raleigh, North Carolina.

21. US Radiology has a number of wholly owned subsidiaries located throughout the country that act on its behalf. One of these subsidiaries is Radiology Ltd., provider of medical imaging services to both Plaintiff Pyle and Plaintiff J-Hanna.

JURISDICTION AND VENUE

22. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's Delaware citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

23. The Court has personal jurisdiction over Defendant because Defendant is incorporated in the State of Delaware, which is coterminous with this District.

24. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant is incorporated in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2).

FACTS

25. Defendant US Radiology Specialists, Inc., is a corporation founded jointly by Charlotte Radiology, a North Carolina based radiology practice, and Welsh, Carson, Anderson, and Stowe, a healthcare investment firm. It describes itself as "building the nation's premier radiology partnership."[1]

26. US Radiology has grown over time by acquiring independent radiology practices across the country. These practices each continue to provide patient care as distinct entities and are referred to by US Radiology as "partner companies."

27. As an umbrella organization, US Radiology works to "share ideas and best

[1] USRADIOLOGY.COM, *Why US Radiology*, www.usradiology.com/why-us-radiology

practices," "invest[] in infrastructure," "execut[e] local and regional growth strategies" and "integrat[e] technology" across its partner companies. [2]

28. In late February of 2022, US Radiology reported a data breach to the U.S. Department of Health and Human Services.

29. Over the next seven months, at least five of US Radiology's subsidiaries sent letters to patients, including Plaintiffs, informing them that their Private Information had been compromised in the Breach. Those five included Gateway Diagnostic Imaging, Radiology Ltd., Charlotte Radiology, Touchstone Medical Imaging, and Diversified Radiology of Colorado.[3] Other subsidiaries may also have sent letters. Charlotte Radiology, in its online notice, also disclosed that patients of its joint venture, Carolinas Imaging Services, LLC, were also impacted by the Data Breach.

30. All of these letters recounted identical facts, and all were signed by Lynn McGiven, US Radiology's Chief Compliance Officer.[4] Each subsidiary reported that an unauthorized party had access to its computer system from December 17, 2021, to December 24, 2021, and that it had

[2] *Id.*

[3] Mont. Dept. of Justice, "Reported Data Breach Incidents," Reported Data Breach Incidents - Montana Department of Justice (dojmt.gov) (search for data breaches with "Start of Breach" as 12/17/2021).

[4] *Compare* Letter from Lynn McGivern on behalf of Radiology Ltd., to affected patients, https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-540.pdf (reported to the Montana Attorney General Sept. 2, 2022); *with* Letter from Lynn McGivern on behalf of Gateway Diagnostic Imaging, https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-539.pdf (reported to the Montana Attorney General Sept. 2, 2022); Letter from Lynn McGivern on behalf of Touchstone Medical Imaging, https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-233.pdf (reported to the Montana Attorney General Feb. 18, 2022); *and* Letter from Lynn McGivern on behalf of Diversified Radiology of Colorado https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-231.pdf (reported to the Montana Attorney General Feb. 18, 2022).

discovered the Breach on December 24, 2021.

31. None of the letters, however, disclosed any relationship between its respective subsidiary and US Radiology. Ms. McGivern signed each letter as simply "Lynn McGivern[,] Privacy Officer."

32. Upon information and belief, the letters from each subsidiary all stem from the Data Breach. Because Defendant "integrate[s] technology" across subsidiaries, an attack on its computer systems would affect patients across multiple subsidiaries.

33. In December of 2021, Defendant discovered unauthorized activity on its computer systems, which contained patients' Private Information, including addresses, dates of birth, health insurance information, medical record numbers, patient account numbers, physician names, dates of service, diagnoses, treatment information related to radiology services, driver's license numbers and Social Security numbers (SSNs).

34. Although Defendant learned of the Data Breach in December 2021, Defendant would only inform patients of the Breach in a piecemeal fashion over the next nine months, through its various subsidiaries.

35. In or around February of 2022, Defendant's subsidiary Charlotte Radiology posted the following notice on its website:[5]

> **Notice of IT Security Incident Affecting Certain Patients**
>
> In late 2021, Charlotte Radiology experienced an incident that involved certain patients' information. We have completed our investigation and there is no evidence that this incident resulted in

[5] *Notice of IT Security Incident Affecting Certain Patients*, https://www.charlotteradiology.com/patient-notice/ (last visited Oct. 7, 2022) [hereinafter *Data Breach Notice*]. For the oldest accessible copy of the notice, see *Archive.org, the Wayback Machine*, "charlotteradiology.com/patient-notice" at https://web.archive.org/web/20220000000000*/www.charlotteradiology.com/patient-notice/ (displaying Feb. 22, 2022).

> fraud or misuse of the information involved. We expect to complete the notification process for all identified individuals by the end of September.
>
> On December 24, 2021, we identified a security incident that impacted systems that contained our patient information. We immediately initiated our incident response process, notified law enforcement, and began an investigation with the assistance of a forensic firm. Within days, we were able to contain the incident and resume serving patients. The investigation subsequently determined that between December 17 and December 24, 2021, an unauthorized party gained access to our network.
>
> Some patients' information may have been accessed, including patient names and one or more of the following: address, date of birth, health insurance information, medical record number, patient account number, physician name, date(s) of service, diagnosis, and/or treatment information related to radiology services. For a limited number of patients, Social Security numbers and/or driver's license numbers may have been included. We are offering complimentary credit monitoring to those individuals.
>
> In addition to caring for our own patients, Charlotte Radiology supervises and manages the operations of Carolinas Imaging Services, LLC (CIS), which provides imaging services in Charlotte, Rock Hill and Huntersville. On April 25, 2022, Charlotte Radiology notified CIS that this security incident impacted certain CIS patients. We recommend that patients review the statements they receive from their health insurer. If you see charges for services you did not receive, please call the insurer immediately.
>
> We have also set up a dedicated call center to answer questions about this incident. Patients with questions may call the call center at 1-855-604-1852, Monday through Friday between 9 AM – 9 PM Eastern Time.
>
> We continue to implement enhancements to information security, systems, and monitoring capabilities and are committed to maintaining the confidentiality and security of patients' information.

36. In September of 2022, nearly nine (9) months after US Radiology discovered the Data Breach, Plaintiff J-Hanna received a letter from Radiology Ltd., a subsidiary of US Radiology and a provider of medical services to her. The letter reads as follows:

Dear Ariann J Hanna:

Radiology Ltd. takes seriously the confidentiality and security of our patients' information. Regrettably, we recently determined that some of your information was involved in a security incident. We have no evidence of fraud or misuse of your information as a result of this incident. However, we are providing information about the incident, the steps we have taken to respond, and the resources we are making available to you.

What Happened: On December 24, 2021, we identified a security incident that impacted systems that contained our patient information. We immediately initiated our incident response process, notified law enforcement, and began an investigation with the assistance of a forensic firm. The investigation determined that between December 17 and December 24, 2021, an unauthorized party gained access to our network.

What Information Was Involved: The information that may have been accessed included your name, and may have included your address, date of birth, health insurance information, medical record number, patient account number, physician name, date(s) of service, and/or information related to radiology services.

What Are We Doing: The safety of your information is of utmost importance to us. To help prevent something like this from happening again, we are continuing to implement additional safeguards and enhancements to our information security, systems, and monitoring capabilities

What You Can Do: We recommend that you review the statements you receive from your health insurer. If you see charges for services you did not receive, please call the insurer immediately.

For More Information: We deeply regret that this incident occurred and for [*sic*] any concern this may cause you. We value your trust and confidence in us and look forward to continuing to serve you. If you have questions about the incident, please call the dedicated call center at 1-855-604-1852, Monday through Friday, between 6:00 a.m. and 6:00 p.m. Pacific Time.
Sincerely,
[*/s/*]
Lynn McGivern
Privacy Officer

37. Plaintiff Pyle also received this form letter.

38. Neither Defendant nor its subsidiaries offered any explanation for the delay between the initial discovery of the Breach and the belated notification to affected patients, delay that resulted in Plaintiffs and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

39. Defendant's notices of the Data Breach, distributed through its various subsidiaries, were not just untimely but woefully deficient, failing to provide basic details, including, but not limited to, how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach occurred system-wide, whether servers storing information were accessed, and how many patients were affected by the Data Breach.

40. Even worse, neither US Radiology nor its subsidiaries offered any remedial services at all to the affected patients. Instead, they offered only one year of credit monitoring to a select few Class members, a measure that is, itself, insufficient to protect against harm that can come about far in the future.

41. In fact, US Radiology left the onus entirely upon its (and its subsidiaries') patients to anticipate, discover, and correct any harms produced by its negligence.

42. In light of the types of Private Information at issue, and the fact that the Private Information was specifically targeted by cybercriminals with the intent to steal and misuse it, it can be determined that Plaintiffs' and Class members' Private Information is being sold on the dark web, meaning that unauthorized parties have accessed, viewed, and exfiltrated Plaintiffs' and Class members' unencrypted, unredacted, sensitive personal information, including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, policy numbers, medical diagnoses and more.

43. The Data Breach occurred because US Radiology failed to take reasonable measures to protect the PII it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the healthcare industry, insurance companies, and associated entities about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers.

44. Defendant disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class members was exfiltrated through unauthorized access by an unknown, malicious cyber hacker with the intent to fraudulently misuse it. Plaintiffs and Class members have a continuing interest in ensuring that their compromised Information is and remains safe.

A. Defendant's Privacy Promises

45. Defendant, by and through its subsidiaries, made and continues to make various promises to its patients, including Plaintiffs, that it will maintain the security and privacy of their Private Information.

46. For example, Radiology Ltd, in its Notice of Privacy Practices (which was applicable to Plaintiffs), in a section titled "Permissible Uses and Disclosures Without Your Written Authorization," describes how it may use and disclose medical information for each category of uses or disclosures. None of them provide it a right to expose patients' Private

Information in the manner in which it was exposed to unauthorized third parties in the Data Breach.[6]

47. By failing to protect Plaintiffs' and Class members' Private Information, and by allowing the Data Breach to occur, US Radiology Specialists broke these promises to Plaintiffs and Class members.

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Subsidiaries' Patients' Private Information

48. US Radiology acquires, collects, and stores a massive amount of its subsidiaries' patients protected PII, including health information and other personally identifiable data.

49. As a condition of engaging in health-related services, US Radiology requires that its subsidiaries entrust it with their patients' highly confidential Private Information.

50. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class members' Private Information, US Radiology assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs and Class members' Private Information from disclosure.

51. Defendant had obligations created by the Health Insurance Portability and Accountability Act (42 U.S.C. § 1320d *et seq.*) ("HIPAA"), industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

52. As evidenced by Defendant's failure to comply with its legal obligations established by HIPAA and Delaware law, Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information.

[6] Radiology Ltd., Notice of Privacy Practices, radltd.com/files/Notice-of-Privacy-Practices-RadLtd-forwebsite.pdf (last accessed Oct. 20, 2022).

53. Plaintiffs and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

54. Prior to and during the Data Breach, Defendant implicitly and explicitly promised patients that their Private Information would be kept confidential, and implicitly and explicitly promised its subsidiaries that their patients' information would be kept confidential.

55. Defendant's failure to provide adequate security measures to safeguard Plaintiffs' and Class members' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to patients' highly confidential Private Information.

56. In fact, Defendant has been on notice for years that the healthcare industry and health insurance companies are a prime target for scammers because of the amount of confidential customer information maintained.

57. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[7]

[7] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warnshealthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

58. The American Medical Association ("AMA") has also warned healthcare companies about the important of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[8]

59. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[9] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[10] That trend continues.

60. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[11] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[12] Almost 50

---

[8] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[9] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[10] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

[11] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, https://www.idtheftcenter.org/2018-data-breaches/.

[12] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[13]

61. A 2017 study conducted by HIMSS Analytics showed that email was the most likely cause of a data breach, with 78 percent of providers stating that they experienced a healthcare ransomware or malware attack in the past 12 months.

62. Healthcare related data breaches continued to rapidly increase into 2021 when US Radiology was breached.[14]

63. In the Healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as "incredible."[15]

64. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[16]

---

[13] *Id.*
[14] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.
[15] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results*, PROOFPOINT (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishingstatistics-2019-himss-survey-results.
[16] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

65. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet

> browsers or compression/decompression programs, including the AppData/LocalAppData folder.
>
> - Consider disabling Remote Desktop protocol (RDP) if it is not being used.
> - Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
> - Execute operating system environments or specific programs in a virtualized environment.
> - Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

66. The threat continues. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for consumers' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).[17]

67. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

> - **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

[17] CONSUMER FIN. PROT. BUREAU, *Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information* (Aug. 11, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-04_circular_2022-08.pdf.

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[18]

[18] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

68. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;

- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

[19] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

69. These are basic, common-sense email security measures that every business, not only healthcare businesses, should be doing. US Radiology, with its heightened standard of care should be doing even more. But by adequately taking these common-sense measures, US Radiology could have prevented this Data Breach from occurring.

70. Charged with handling sensitive Private Information, including healthcare information, Defendant knew, or should have known, the importance of safeguarding its subsidiaries' patients' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on its subsidiaries' patients as a result of a breach. US Radiology failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

71. With respect to training, Defendant specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

72. The Private Information was also maintained on US Radiology's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's systems through ransomware attacks. US Radiology also kept the data of its subsidiaries' patients on a common computer system, such that a data breach that compromised the security of one subsidiary would compromise others, as well. The mechanism of the cyberattack and the potential for improper disclosure of Plaintiffs and Class members' PII was a known risk to US Radiology, and

thus US Radiology was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information

73. The fact that Plaintiffs and Class members' Private Information was stolen means that Class members' information is likely for sale by cybercriminals and will be misused in additional instances in the future.

74. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiffs and Class members is highly sensitive and of significant value to those who would use it for wrongful purposes.

75. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[20] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive health information on multiple underground Internet websites, commonly referred to as the dark web.

76. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[21]

---

[20] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

21 *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

77. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[22]

78. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> 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.[23]

79. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[24] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

80. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their

---

[22] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

[23] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

24 *Web's Hot New Commodity*, *supra* note 17.

data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[25]

81. The value of Plaintiffs and Class members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[26] This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

82. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[27]

83. The ramifications of US Radiology's failure to keep its patients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

---

25 *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

26 Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.

27 Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.

84. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[28] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[29]

85. Breaches are particularly serious in healthcare industries. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[30] Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[31] Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[32]

---

[28] *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[29] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[30] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, (2019) https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[31] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

[32] *Id.*

86. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks, given the significant number of data breaches affecting the health care industry and related industries.

87. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into its systems and, ultimately, the theft of its patients' Private Information.

88. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[33] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[34] Based upon information and belief, the unauthorized parties utilized the Private Information they

[33] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[34] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

obtained through the Data Breach to obtain additional information from Plaintiffs and Class members that was misused.

89. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

90. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information was not involved in the Data Breach, the unauthorized parties could use Plaintiffs and Class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

91. Given these facts, any healthcare or other type of entity that transacts business with patients or customers and then compromises the privacy of its patients' or customers' Private Information has thus deprived them of the full monetary value of the transaction with the entity.

92. Acknowledging the damage to Plaintiffs and Class members, Defendant instructed patients like Plaintiff to "review the statements you receive from your health insurer" and call the insurer "immediately" if fraudulent charges appear. Plaintiffs and Class members now face an impending, substantial risk of identity theft and medical insurance fraud.

93. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

D. US Radiology's Conduct violated HIPPA

94. HIPAA requires covered entities like US Radiology to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[35]

95. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

96. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[36]

97. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. US Radiology's security failures include, but are not limited to, the following:

- Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

- Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

[35] *What is Considered Protected Health Information Under HIPAA*?, HIPPA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.
[36] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

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

- Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

- Failing to protect 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);

- Failing to protect against any reasonably anticipated uses or disclosures of electronically 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);

- Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. §164.306(a)(94);

- Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

- Failing to effectively train all members of its workforce (including agents and independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

- Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

E. US Radiology Specialists Failed to Comply with FTC Guidelines

98. US Radiology was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to

maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

99. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[37]

100. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[38] 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 to correct any security problems.

101. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[39]

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

---

[37] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

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

[39] *Start with Security*, *supra* note 32.

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

103. US Radiology was at all times fully aware of its obligation to protect the Private Information of its patients. US Radiology was also aware of the significant repercussions that would result from its failure to do so.

104. As evidenced by Defendant's failure to comply with its legal obligations established by the FTC Act, Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information

F. US Radiology Failed to Comply with Healthcare Industry Standards

105. HHS's Office for Civil Rights has stated:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[40]

106. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

[40] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.

107. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because the of the value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[41] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

108. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, US Radiology chose to ignore them. These best practices were known, or should have been known by US Radiology, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

G. Damages to Plaintiffs and the Class

109. Plaintiffs and the Class have been damaged by the compromise of their Private Information in the Data Breach.

110. The ramifications of US Radiology's failure to keep its patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[42]

111. In addition to its obligations under state and federal laws and regulations, Defendant owed a common law duty to Plaintiffs and Class members to protect the Private Information they entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding,

[41] *See, e.g.*, *10 Best Practices For Healthcare Security*, INFOSEC, https://resources.infosecinstitute.com/topics/healthcare-information-security/#gref.
[42] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

112. Defendant further owed and breached its duty to Plaintiffs and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

113. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiffs and Class members' Private Information as detailed above, and Plaintiffs and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

114. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

115. Some of the injuries and risks associated with the loss of personal information have already manifested themselves in Plaintiffs and other Class members' lives. Each Plaintiff received a cryptically written notice letter from Defendant stating that their Private Information was released, and that they should remain vigilant for fraudulent activity, with no other explanation of where this Information could have gone, or who might have access to it.

116. Plaintiffs and the Class face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, applications for benefits made fraudulent in their names, loans opened in their names, medical services billed in their names, government benefits fraudulently drawn in their name, and identity theft. Many Class members may already be victims of identity theft and fraud without realizing it.

117. For Plaintiff Pyle in particular, these harms are not theoretical. She was billed approximately two hundred fifty-six dollars ($256.00) on or around August 19, 2022, for medical services she never received. The putative bill claimed that she had received a brain scan in April 2022, but her last brain scan had been administered in or around June 2021. Then, in September 2022, she received an invoice for approximately ninety-five dollars ($95.00) for unspecified medical services, which she did not pay. Within the month, that ninety-five-dollar debt had been sent to a collection agency, which negatively impacted her credit. Among other harms, her lower credit score, through no fault of her own, has prompted Plaintiff Pyle to delay purchasing a home, something she has long looked forward to and planned for.

118. Plaintiffs and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

119. Plaintiffs and Class members did not receive the full benefit of their bargain when paying for medical services, and instead received services that were of a diminished value to those described in their agreements with their respective healthcare institutions that had made agreements with US Radiology for the benefit and protection of Plaintiffs and Class members and their respective Private Information. Plaintiffs and Class members were damaged in an amount at

least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

120. Plaintiffs and Class members would not have obtained services from their medical providers had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

121. Plaintiffs and the Class will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

122. The theft of Social Security numbers, which were purloined as part of this Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[43] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[44] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[45]

123. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not

43 *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.
44 *Id.*
45 *Id.*

associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[46]

124. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the healthcare industry context, Private Information can be used to submit false insurance claims. As a result, Plaintiffs and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit for an indefinite duration. For Plaintiffs and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

125. As a result of the Data Breach, Plaintiffs and Class members' Private Information has diminished in value.

126. The Private Information belonging to Plaintiffs and Class members is private and was left inadequately protected by Defendant who did not obtain Plaintiffs or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed Plaintiffs and Class members' Private Information as a direct result of its inadequate security measures.

127. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiffs and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations,

[46] *Id.*

industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

128. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

129. Defendant did not properly train its employees, particularly its information technology department, to timely identify and/or avoid ransomware attacks.

130. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs and Class members' Private Information.

131. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

132. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[47]

[47] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

133. Other than offering 12 months of credit monitoring to a limited subset of Class members, Defendant did not take any measures to assist Plaintiffs and Class members. It simply told them to remain vigilant for incidents of fraud and identity theft. Some of Defendant's subsidiaries may also have advised Class members to review account statements and monitor credit reports for unauthorized activity; obtain a copy of free credit reports; contact the FTC and/or the state Attorney General's office; enact a security freeze on credit files; or create a fraud alert, although Plaintiffs received none of those additional recommendations. None of these suggested measures, however, require Defendant to expend any effort to protect Plaintiffs and Class members' Private Information.

134. Defendant's failure to adequately protect Plaintiffs and Class members' Private Information has resulted in Plaintiffs and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as multiple US Radiology subsidiaries' Data Breach notices have indicated, it and its subsidiaries are putting the burden on Plaintiffs and Class members to discover possible fraudulent activity and identity theft.

135. While Defendant offered one year of credit monitoring to a limited subset of Class members, the credit monitoring offered does not guarantee privacy or data security for Plaintiffs. Thus, to mitigate harm, Plaintiffs and Class members are now burdened with indefinite monitoring and vigilance of their accounts.

136. Moreover, those Class members who have not been offered credit monitoring, such as Plaintiff J-Hanna, are completely and entirely burdened with attempting to mitigate the harms of this Data Breach on their own.

137. Worse still, the limited offer of credit monitoring to only a subset of Class members is woefully inadequate. While some harm has already taken place, the worst is yet to come. There may be a time lag between when harm occurs versus when it is discovered, and between when Private Information is acquired and when it is used. Furthermore, identity theft monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[48] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

138. Plaintiffs and Class members have been damaged in several other ways as well. Plaintiff and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiffs and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming task. Class members have also been forced to purchase adequate credit reports, credit monitoring and other identity protection services, and have placed credit freezes and fraud alerts on their credit reports, while also spending significant time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class members also suffered a loss of the inherent value of their Private Information.

139. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further

[48] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

140. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;
- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members; and
- Anxiety and distress resulting fear of misuse of their Private Information.

141. In addition to a remedy for the economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

142. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and/or 23(c)(4).

143. Specifically, Plaintiffs propose the following Nationwide Class and Arizona Subclass (collectively, the "Class") definitions:

> **Nationwide Class**
> All persons residing in the United States whose Private Information was compromised as a result of the Data Breach discovered on or about December of 2021 and who were sent notice of the Data Breach.
>
> **Arizona Subclass**
> All persons residing in Arizona whose Private Information was compromised as a result of the Data Breach discovered on or about December 2021 and who were sent notice of the Data Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

144. Plaintiffs reserve the right to modify, change, amend, or expand the definitions of the Nationwide Class and Arizona Subclass based upon discovery and further investigation.

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

146. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. Upon information and belief, the Class numbers number in the tens of thousands. Moreover, the Class is composed of an easily ascertainable set of individuals and entities who were patients of Defendant

or its subsidiaries and who were impacted by the Data Breach of Defendant's systems. The precise number of Class members can be further confirmed through discovery, which includes Defendant's records. The disposition of Plaintiffs' and Class members' claims through a class action will benefit the parties and this Court.

147. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiffs' and the Class's Private Information from unauthorized capture, dissemination, and misuse;
- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiffs' and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;
- Whether Defendant was unjustly enriched by its actions; and

- Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

148. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

149. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured and sustained similar monetary and economic injuries as a result of Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to either Plaintiff.

150. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

151. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

152. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy,

and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

153. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

a. The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class members would create a risk of adjudication that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests; and

c. Defendant has acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief with respect to the members of the Class as a whole.

154. Class certification is also appropriate because this Court can designate particular claims or issues for class-wide treatment and may designate multiple subclasses pursuant to Fed. R. Civ. P. 23(c)(4).

155. No unusual difficulties are likely to be encountered in the management of this action as a class action.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclass)

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

157. Upon Defendant's acceptance and storage of the Private Information of Plaintiffs and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that Information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

158. Defendant owed a duty of care not to subject Plaintiffs and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

159. Defendant owed numerous duties to Plaintiffs and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

160. Defendant also breached its duty to Plaintiffs and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs and Class members' Private Information for the purpose of misusing and intentionally disclosing it to others without consent.

161. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.

162. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs and Class members' Private Information.

163. Defendant breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

164. Because Defendant knew that a breach of its systems would damage thousands of its patients, including Plaintiffs and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

165. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class members, which is recognized by laws and regulations including but not limited to common law. Defendant was

in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

166. In addition, Defendant had a duty to employ 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.

167. Defendant also had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

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

169. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiffs and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

170. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice

of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

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

e. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

171. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiffs and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs and Class members' Private Information during the time it was within Defendant's possession or control.

172. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing to provide Plaintiffs and Class members with timely notice that their sensitive Private Information had been compromised.

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

174. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

175. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
BREACH OF THID PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclass)

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

177. US Radiology Specialists entered into various contracts to provide information processing services and "technology integration" to its subsidiaries and "partner companies."

178. The contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential medical information that US Radiology agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

179. US Radiology knew that if it were to breach these contracts with its subsidiaries and partner companies, their patients, including Plaintiffs and the Class, would be harmed by, among other harms, fraudulent transactions.

180. US Radiology breached its contracts with its partner entities affected by the Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

181. As foreseen, Plaintiffs and the Class were harmed by US Radiology's failure to use reasonable security measures to store patient information, including but not limited to the risk of harm through the loss of their personal information.

182. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclass)

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

184. Plaintiffs bring this claim in the alternative to their breach of third-party beneficiary contract claim.

185. Through their course of conduct, Defendant and its subsidiaries, Plaintiffs, and Class members entered into implied contracts for the provision of healthcare and data administration services, as well as implied contracts for the implementation of data security adequate to safeguard and protect the privacy of Plaintiffs and Class members' Private Information.

186. Specifically, Plaintiffs and Class members entered into valid and enforceable implied contracts with Defendant and its subsidiaries when they first entered into the medical claims and billing contracts with Defendant's subsidiaries, including Radiology Ltd., which were acting as Defendant's agent and/or alter ego.

187. The valid and enforceable implied contracts to provide radiology services that Defendant entered into with Plaintiffs and Class members by and through Defendant's subsidiaries or "partner companies" entered into with Defendant include Defendant's promise to protect

nonpublic Private Information given to Defendant or that Defendant created on its own from disclosure.

188. When Plaintiffs and Class members provided their Private Information to Defendant in exchange for services from Defendant and its agents, they entered into implied contracts pursuant to which Defendant agreed to reasonably protect such Information.

189. Defendant, by and through its subsidiaries, solicited and invited Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class members accepted Defendant's offers and provided their Private Information to Defendant.

190. By entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

191. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

192. Under these implied contracts, Defendant was obligated to: (a) provide radiological services to Plaintiffs and Class members; and (b) protect Plaintiffs and Class members' Private Information provided to obtain the benefits of such services. In exchange, Plaintiffs and members of the Class agreed to pay money for these services, and to turn over their Private Information.

193. Both the provision of medical billing and claims services and the protection of Plaintiffs and Class members' Private Information were material aspects of these implied contracts.

194. The implied contracts for the provision of technological services include the contractual obligations to maintain the privacy of Plaintiffs and Class members' Private

Information, which are also acknowledged, memorialized, and embodied in multiple documents (including, among other documents, Defendant's Data Breach notification letter and Defendant's Notice of Privacy Practices).

195. Defendant's express representations, including, but not limited to the express representations found in its Notice of Privacy Practices, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class members' Private Information.

196. Consumers of medical services value their privacy, the privacy of their dependents, and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiffs and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected; nor would they have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

197. A meeting of the minds occurred, as Plaintiffs and Class members agreed and provided their Private Information to Defendant and/or its affiliated healthcare providers and paid for the provided claims review and billing services in exchange for, among other things, both the provision of healthcare and the protection of their Private Information.

198. Plaintiffs and Class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

199. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated through the Data Breach.

200. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiffs and Class members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA or HIPPA, or otherwise protect Plaintiffs and Class members' private information as set forth above.

201. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

202. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class members, therefore, were damaged in an amount at least equal to the difference in the value between the healthcare with data security protection they paid for and the healthcare they received.

203. Had Defendant disclosed that its data security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, Class members, nor any reasonable person would have purchased healthcare services from Defendant's affiliated providers, from which services Defendant directly benefits.

204. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future,

disruption of their medical care and treatment, out of pocket expenses to mitigate the effects of the Data Breach, including time lost responding to the Breach, and the loss of the benefit of the bargain they struck with Defendant.

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

206. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclass)

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

208. In providing their Private Information to Defendant, Plaintiffs and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard for the interests of Plaintiffs and Class members to safeguard and keep confidential that Private Information.

209. Defendant accepted the special confidence Plaintiffs and Class members placed in it, as evidenced by its assertion that it is "committed to protecting the privacy of [Plaintiffs'] personal information" as included in the form Data Breach notification letters that its Chief Compliance Officer distributed to Class members through its subsidiaries.

210. In light of the special relationship between Defendant and Plaintiffs and Class members, whereby Defendant became a guardian of Plaintiffs and Class members' Private

Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class members for the safeguarding of Plaintiffs and Class members' Private Information.

211. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of its customer relationships, in particular, to keep secure the Private Information of its patients.

212. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to protect the integrity of the systems containing Plaintiffs and Class members' Private Information.

213. Defendant breached its fiduciary duties to Plaintiffs and Class members by otherwise failing to safeguard Plaintiffs and Class members' Private Information.

214. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder

of the lives of Plaintiffs and Class Members; and (vii) the diminished value of the services they paid for and received.

215. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
DECLARATORY RELIEF
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Arizona Subclass)

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

217. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

218. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that additional compromises of their PII will occur in the future.

219. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

220. Defendant still possesses the PII of Plaintiffs and the Class.

221. Defendant has made no announcement that it has changed its data storage or security practices relating to the storage of Plaintiffs' and Class members' PII.

222. To Plaintiffs' knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

223. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at US Radiology. The risk of another such breach is real, immediate, and substantial.

224. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at US Radiology, Plaintiffs and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

225. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at US Radiology, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other consumers whose PII would be further compromised.

226. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that US Radiology Specialists implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on US Radiology's systems on a periodic basis, and ordering US Radiology to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

e. conducting regular database scans and security checks; and

f. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in favor of Plaintiffs and the Class and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and

Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for no less than three (3) years of credit monitoring services for Plaintiffs and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Dated: October 21, 2022

/s/ P. Bradford deLeeuw
P. Bradford deLeeuw (#3569)
DELEEUW LAW LLC
1301 Walnut Green Road
Wilmington, DE 19807
(302) 274-2180
brad@deleeuwlaw.com

OF COUNSEL

Nicholas A. Migliaccio
Jason S. Rathod
Tyler J. Bean
MIGLIACCIO & RATHOD, LLP
412 H Street, NE, Suite 302
Washington, DC 20002
Phone: 202-470-520
Fax: 202-800-2730
Email: nmigliaccio@classlawdc.com

Attorneys for Plaintiffs and the Putative Class

ClassAction.org