UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

Gerald Lee, individually and on behalf of all similarly situated individuals, Plaintiff, v. QRS, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Gerald Lee, ("Plaintiff"), individually and on behalf of all other similarly situated individuals, and by and through his undersigned counsel files this Class Action Complaint against QRS, Inc. ("QRS") ("Defendant"), and alleges the following based upon personal knowledge of facts pertaining to Gerald Lee and upon information and belief based upon the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused him and the nearly 320,000 similarly situated persons in the massive and preventable data breach that took place between August 23, 2021 and August 26, 2021 by which cyber criminals, through a phishing event, infiltrated Defendant's inadequately protected QRS server, more specifically the QRS patient portal, where sensitive personal information was being kept unprotected ("Data Breach" or "Breach").[1]

[1]The Data Breach appears on the U.S. Department of Health and Human Services' online public breach tool and shows that approximately 319,778 individuals were affected by the Data Breach. *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Dec. 22, 2021).

2. The cyber criminals gained access to certain of Defendant's patient portal with the apparent intention of stealing protected personal information and protected health information of hundreds of thousands of individuals, whose information was stored on Defendant's computer systems and in Defendant's patient portal.

3. QRS is practice management software organization that partners health care providers and medical services organizations to offer a "practice management suite that includes: Patient Management, Patient Scheduling, Professional Billing, Institutional Billing, Guarantor Billing, Electronic Billing, Electronic Remittance, HL7-Interfaces, Claims Error Information System, as well as specialty specific options."[2]

4. QRS collaborates with its partners and affiliates "to provide creative software and hardware solutions using modern computer technology, provide friendly customer driven implementation, and training and support of these products as well as a full line of services to supplement these products[,]" and touts on its website that its goal is to "unburden you from the technical and administrative responsibilities of managing your practice" by providing the "best software and hardware products."[3] The experience QRS provides includes "programmers and network engineers." [4]

5. Plaintiff and Class members are required, as patients of medical providers who utilize Defendant's software, to provide Defendant with their "Personal and Medical Information" (defined below), with the assurance that such information will be kept safe from unauthorized access. By taking possession and control of Plaintiff's and Class members' Personal and Medical

[2] https://www.qrshs.com/about/ (last accessed Dec. 22, 2021).
[3] *Id*.
[4] *Id*.

Information, Defendant assumed a duty to securely store the Personal and Medical Information of Plaintiff and the Class.

6. Defendant breached this duty and betrayed the trust of Plaintiff and Class members by failing to properly safeguard and protect their Personal and Medical Information, thus enabling cyber criminals to steal it.

7. Information compromised in the Data Breach includes the following information belonging to current and former patients of healthcare providers that employed QRS: names, Social Security numbers, dates of birth, patient numbers, portal usernames, addresses, and limited medical treatment and diagnosis information (collectively the "Personal and Medical Information"). In addition, compromised information may include other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that QRS collected and maintained through the electronic patient portals it maintained for its clients.[5]

8. Defendant's misconduct – failing to timely implement adequate and reasonable measures to protect Plaintiff's Personal and Medical Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices in place to safeguard the Personal and Medical Information, failing to honor its promises and representations to protect Plaintiff's and Class members' Personal and Medical Information, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiff and Class members across the United States.

[5] https://www.databreaches.net/?s=QRS (last accessed Dec. 22, 2021.)

9. Due to Defendant's negligence and failures, cyber criminals obtained and now possess everything they need to commit personal and medical identity theft and wreak havoc on the financial and personal lives of nearly 320,000 individuals for decades to come.

10. As a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that their Personal and Medical Information has been released into the criminal cyber domains, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class members are now forced to deal with the danger of identity thieves possessing and using their Personal and Medical Information. Additionally, Plaintiff and Class members have already lost time and money responding to and mitigating the impact of the Data Breach.

11. Plaintiff brings this action individually and on behalf of the Class and seeks actual damages, statutory damages, punitive damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security systems and protocols), reasonable attorney fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems proper.

THE PARTIES

Plaintiff Gerald Lee

12. Gerald Lee is and at all times mentioned herein, an individual citizen and resident of South Carolina.

13. Plaintiff received a letter from QRS dated October 22, 2021, informing him that his name, Social Security Number, date of birth, patient number, portal username, and address and medical treatment and diagnosis information, in the Data Breach. *See* **Exhibit 1**, the "Notice."

14. As required to obtain medical services, Plaintiff was required to input highly sensitive personal, health, and insurance information (Personal and Medical Information compromised in the Data Breach) into Defendant's patient portal. Plaintiff believes this is a standard practice required of all providers that utilize Defendant's software.

15. Because of Defendant's negligence leading to the Data Breach, Plaintiff's Personal and Medical Information is now in the hands of cyber criminals and Plaintiff is now under imminent risk of identity theft and fraud, including medical identity theft and medical fraud.

16. The imminent risk of medical identity theft and fraud that Plaintiff now faces is substantial, certainly impending, and continuous and ongoing because of the negligence of Defendant, the same negligence which led to the Data Breach. Plaintiff has already been forced to spend time and money responding to the Data Breach in an attempt to mitigate the harms of the Breach and determine how best to protect himself from identity theft and medical information fraud. These efforts are continuous and ongoing.

17. As a direct and proximate result of the Data Breach, Plaintiff has had to purchase a yearly subscription to identity theft protection and credit monitoring in order to protect himself from medical identity theft and other types of fraud of which he is now substantially at risk. This subscription will need to be renewed yearly for the rest of Plaintiff's lifetime.

18. Plaintiff has suffered an increase in spam and phishing emails and U.S. mail. Some of the increased spam and phishing include repugnant "Adult" websites ads.

19. Plaintiff has also suffered from spam and phishing responses on his business advertisements which has resulted in Plaintiff having to spend time and money filtering out spam and phishing responses and missing legitimate business opportunities. In addition, Plaintiff has spent time and money to delete advertisements and create new advertisements.

20. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including damages and diminution in value of his Personal and Medical Information that was entrusted to Defendant for the sole purpose of obtaining medical services necessary for his health and well-being, with the understanding that Defendant would safeguard this information against disclosure. Additionally, Plaintiff's Personal and Medical Information is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect it.

21. For the avoidance of doubt, all references made in this Complaint to "Plaintiff's Personal and Medical Information" are to be interpreted as referring to Gerald Lee's Personal and Medical Information.

Defendant QRS

22. Defendant QRS Inc. is a Tennessee corporation with its headquarters and principal place of business at 2010 Castaic Ln, Knoxville, TN 37932-1557.

23. Founded in 1983, Defendant provides a full suite of practice management solutions to healthcare providers, including a patient portal that stores patient's personal and medical information.

JURISDICTION AND VENUE

24. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class are citizens of states that differ from Defendant.

25. This Court has jurisdiction over the Defendant because it operates and/or is incorporated in this District, and the computer systems implicated in this Data Breach are likely based in this District.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendant is based in this District, maintains Class members' Personal Medical Information in this District and have caused harm to Class members residing in this District.

FACTUAL ALLEGATIONS

A. The Data Breach and Defendant's Failed Response

27. On August 26, 2021, QRS discovered that a cyber-attacker accessed one QRS dedicated patient portal server and may have acquired certain personal information stored on that specific server.

28. Upon discovering the attack, QRS took the server offline, began an investigation, and notified law enforcement.

29. QRS also engaged a forensic security firm to assess the security of its network, analyze the incident, and determine the extent of the personal information that may have been accessed or acquired by the third party.

30. The investigation determined that the attacker accessed the single server from August 23, 2021, to August 26, 2021.

31. During this time, the attacker accessed, and likely acquired, files on the server that contained certain individuals' personal information. The information may have included, depending on the individual, their name, address, date of birth, Social Security number, patient identification number, portal username, and/or medical treatment or diagnosis information.

32. The Data Breach remains under investigation by the U.S. Department of Health and Human Services' Office for Civil Rights.

33. Plaintiff's and Class members' Personal and Medical Information was accessed and stolen in the Data Breach.

34. Upon information and belief, the unauthorized third-party gained access to the Personal and Medical Information and has engaged in (and will continue to engage in) misuse of the Personal and Medical Information, including marketing and selling Plaintiff's and Class members' Personal and Medical Information on the dark web.

35. QRS first notified its health provider clients of the incident. On October 22, 2021, on behalf of QRS's clients, QRS began sending written notifications to individuals whose personal information was accessed by the attacker and for whom QRS has contact information.

36. Apparently, Defendant chose to complete its investigation and develop a list of talking points before giving Plaintiff and Class members the information they needed to protect themselves against fraud and identity theft.

37. Despite the severity of the Data Breach, Defendant has done very little to protect Plaintiff and the Class. In the Notice, Defendant does not provide any suggestions to protect the victims and merely offers a free credit reporting service.[6]

38. In effect, Defendant is shirking its responsibility for the harm and increased risk of harm it has caused Plaintiff and members of the Class, including the distress and financial burdens the Data Breach has placed upon the shoulders of the Data Breach victims.

[6] *See* **Exhibit 1.**

39. Defendant failed to adequately safeguard Plaintiff's and Class members' Personal and Medical Information, allowing cyber criminals to access this wealth of priceless information for nearly two months before warning the criminals' victims to be on the lookout.

40. Defendant failed to spend sufficient resources on monitoring its own software platform it built and training its employees to identify cyber threats and defend against them.

41. Defendant had obligations created by the Health Insurance Portability and Accountability Act ("HIPAA"), reasonable industry standards, common law, state statutory law, and their assurances and representations to their patients to keep patients' Personal and Medical Information confidential and to protect such Personal and Medical Information from unauthorized access.

42. Plaintiff and Class members were required to provide their Personal and Medical Information to Defendant with the reasonable expectation and mutual understanding that it would comply with its obligations to keep such information confidential and secure from unauthorized access.

43. The stolen Personal and Medical Information at issue has great value to the hackers, due to the large number of individuals affected and the fact that health insurance information and Social Security numbers were part of the data that was compromised.

B. Defendant had an Obligation to Protect Personal and Medical Information under Federal Law and the Applicable Standard of Care

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

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

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

47. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

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

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

a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

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

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

d) Ensure compliance by their workforce.

50. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

51. HIPAA also requires Defendant to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

52. Defendant were also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "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).

53. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal and Medical Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Personal and Medical Information of the Class.

54. Defendant owed a duty to Plaintiff and the Class to design, maintain, and test its computer and email systems to ensure that the Personal and Medical Information in Defendant's possession was adequately secured and protected.

55. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the Personal and Medical Information in its possession, including adequately training their employees and others who maintained and

accessed Personal Information within its computer systems on how to adequately protect Personal and Medical Information.

56. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a breach on its data security systems in a timely manner.

57. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

58. Defendant owed a duty to Plaintiff and the Class to adequately train and supervise its employees to identify and avoid any cyber intrusion on its system.

59. Defendant owed a duty to Plaintiff and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal and Medical Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal and Medical Information with Defendant.

60. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

61. Defendant owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

C. Defendant was on Notice of Cyber Attack Threats in the Healthcare Industry and of the Inadequacy of their Data Security

62. Defendant was on notice that companies in the healthcare industry were targets for cyberattacks.

63. Defendant was on notice that the FBI has recently 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]

64. The American Medical Association ("AMA") has also warned healthcare companies about the importance 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]

65. As implied by the above quote from the AMA, stolen Personal and Medical Information can be used to interrupt important medical services themselves. This is an imminent and certainly impending risk for Plaintiff and Class members.

66. Defendant was on notice that the federal government has been concerned about healthcare company data encryption. Defendant knew it kept protected health information in its patient portal and yet it appears Defendant did not adequately safeguard its systems.

67. Defendant owed a duty to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

---

[7] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[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-ransomeware-attacks-shut-down-clinics-hospitals.

68. As covered entities or business associates under HIPAA, Defendant should have known about its weakness toward the patient portal threats and sought better protection for the Personal and Medical Information on the platform which it built and maintained.

69. QRS's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

70. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[9]

71. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[10]

72. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years. For instance, the 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[11]

73. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[12]

74. In 2021 alone there have been over 220 data breach incidents. These approximately 220 data breach incidents have impacted nearly 15 million individuals.

[9] *See* https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 23, 2021).
[10] *Id.*
[11] *Id.*
[12] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

75. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

76. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."[13]

77. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in QRS's industry, including QRS.

D. Cyber Criminals Will Use Plaintiff's and Class Members' Personal and Medical Information to Defraud Them

78. Plaintiff and Class members' Personal and Medical Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune.

79. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[14] For example, with the Personal and Medical Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government

[13] *See* https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last accessed Dec. 23, 2021).

[14] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[15] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class members.

80. Personal and Medical Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[16]

81. For example, it is believed that certain Personal and Medical Information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits in various states across the U.S.[17]

82. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off of the sale of Plaintiff's and the Class members' Personal and Medical Information on the dark web. The Personal and Medical Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

83. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[18]

84. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies

---

[15] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[16] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu

[17] *See https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/

[18] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

85. For instance, with a stolen Social Security number, which is part of the Personal and Medical Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[20] Identity thieves can also use the information stolen from Plaintiff and Class members to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

86. Medical identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[21]

87. "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."[22]

88. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit

[19] *Data Breaches Are Frequent*, *supra* note 11.
[20] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.
[21] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.
[22] *Id.*

cards can be, say, five dollars or more where [personal health information] can go from $20 say up to—we've seen $60 or $70 [(referring to prices on dark web marketplaces)]."[23] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[24]

89. If cyber criminals manage to steal financial information, health insurance information, and driver's licenses—as they did here—there is no limit to the amount of fraud to which Defendant has exposed the Plaintiff and Class members.

90. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[25] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[26]

91. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[27]

92. Defendant's offer of one year of identity theft monitoring is, in and of itself, woefully inadequate, as the worst is yet to come.

---

[23] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowedge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[24] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[25] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[26] *Id.*; *see also Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[27] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

93. With this Data Breach, it is likely identity thieves have already started to prey on the victims, and we can anticipate that this will continue.

94. Victims of the Data Breach, like Plaintiff and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[28]

95. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

96. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a) Trespass, damage to, and theft of their personal property including Personal and Medical Information;

b) Improper disclosure of their Personal and Medical Information;

c) The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal and Medical Information being placed in the hands of criminals and having been already misused;

[28] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

d) The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

e) Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f) Loss of privacy suffered as a result of the Data Breach;

g) Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h) Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i) The loss of use of and access to their credit, accounts, and/or funds;

j) Damage to their credit due to fraudulent use of their Personal and Medical Information; and

k) Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

97. Moreover, Plaintiff and Class members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiff's and Class members' Personal and Medical Information.

98. Plaintiff and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the kind of Personal and Medical Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves

have their Personal and Medical Information, Plaintiff and all Class members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[29]

99. None of this should have happened. The Data Breach was preventable.

E. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' Personal and Medical Information

100. Data breaches are preventable.[30] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[31] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[32]

101. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[33]

102. Defendant required Plaintiff and Class members to surrender their Personal and Medical Information – including but not limited to their names, addresses, Social Security numbers, medical information, and health insurance information – and were entrusted with

---

[29] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.
[30] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[31] *Id.* at 17.
[32] *Id.* at 28.
[33] *Id.*

properly holding, safeguarding, and protecting against unlawful disclosure of such Personal and Medical Information.

103. Defendant breached fiduciary duties owed to Plaintiff and the Class and guardians of Plaintiff's and Class members' Personal and Medical Information.

104. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiff's and Class members' Personal and Medical Information.

105. Defendant maintained the Personal and Medical Information in a reckless manner.

106. Defendant knew, or reasonably should have known, of the importance of safeguarding Personal and Medical Information and of the foreseeable consequences that would occur if Plaintiff's and Class members' Personal and Medical Information was stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of a breach.

107. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class members' Personal and Medical Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class members' Personal and Medical Information from those risks left that information in a dangerous condition.

108. Defendant disregarded the rights of Plaintiff and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' Personal and Medical Information;

(iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

CLASS ACTION ALLEGATIONS

109. Plaintiff brings this action against Defendant on behalf of himself and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of the Class and Subclass defined as follows:

Nationwide Class

> **All persons residing in the United States whose personal and medical information was compromised as a result of the QRS Data Breach that occurred in August 2021.**

South Carolina Subclass

> **All persons residing in South Carolina whose personal and medical information was compromised as a result of the QRS Data Breach that occurred in August 2021.**

110. Excluded from the Nationwide Class and Subclass are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

111. Plaintiff reserves the right to amend the above definitions or to propose alternative or additional subclasses in subsequent pleadings and motions for class certification.

112. The Nationwide Class and the South Carolina Subclass are collectively referred to as the "Class" unless otherwise specified.

a. Class Certification is Appropriate

113. The proposed Class and Subclass meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

114. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable. The proposed Subclass is also believed to be so numerous that joinder of all members would be impractical.

115. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive Personal and Medical Information compromised in the same way by the same conduct of Defendant.

116. **Adequacy:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class and proposed Subclass that he seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

117. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay

and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

118. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant engaged in the wrongful conduct alleged herein;

b) Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Personal and Medical Information;

c) Whether Defendant's servers, software, and computer systems and data security practices used to protect Plaintiff's and Class members' Personal and Medical Information violated the FTC Act and/or HIPAA, and/or state laws and/or Defendant's other duties discussed herein;

d) Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Personal and Medical Information, and whether it breached this duty;

e) Whether Defendant knew or should have known that their systems and servers were vulnerable to a data breach;

f) Whether Defendant's conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach;

g) Whether Defendant breached contractual duties to Plaintiff and the Class to use reasonable care in protecting their Personal and Medical Information;

h) Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i) Whether Defendant continue to breach duties to Plaintiff and the Class;

j) Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

k) Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

l) Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class;

m) Whether Defendant's actions alleged herein constitute gross negligence; and

n) Whether Plaintiff and Class members are entitled to punitive damages.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class or, alternatively, Plaintiff and the South Carolina Subclass)

119. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

120. Defendant gathered and stored the Personal and Medical Information of Plaintiff and the Class as part of the operation of its business.

121. Upon accepting and storing the Personal and Medical Information of Plaintiff and Class members, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

122. Defendant had full knowledge of the sensitivity of the Personal and Medical Information, the types of harm that Plaintiff and Class members could and would suffer if the Personal and Medical Information was wrongfully disclosed, and the importance of adequate security.

123. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their Personal and Medical Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

124. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal Personal and Medical Information.

125. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

126. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

127. Defendant had duties to protect and safeguard the Personal and Medical Information of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-

sense precautions when dealing with sensitive Personal and Medical Information. Additional duties that Defendant owed Plaintiff and the Class include:

a) To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' Personal and Medical Information was adequately secured from impermissible release, disclosure, and publication;

b) To protect Plaintiff's and Class members' Personal and Medical Information in their possession by using reasonable and adequate security procedures and systems;

c) To implement processes to quickly detect a data breach, security incident, or intrusion involving their client portal and other systems, networks and servers; and

d) To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal and Medical Information.

128. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Personal and Medical Information that Plaintiff and the Class had entrusted to it.

129. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class members' Personal and Medical Information. Defendant breached its duties by, among other things:

a) Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Personal and Medical Information in its possession;

b) Failing to protect the Personal and Medical Information in its possession using reasonable and adequate security procedures and systems;

c) Failing to adequately and properly audit, test, and train its employees to detect, build, and implement secure systems on its client portal and other platforms;

d) Failing to use adequate security systems, including healthcare industry standard cybersecurity protocols.

e) Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Personal and Medical Information;

f) Failing to adequately train its employees to not store Personal and Medical Information in longer than absolutely necessary for the specific purpose that it was sent or received;

g) Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's Personal and Medical Information;

h) Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

i) Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their Personal and Medical Information.

130. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

131. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

132. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Personal and Medical Information of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Personal and Medical Information of Plaintiff and Class members while it was within Defendant's possession and control.

133. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to securing their Personal and Medical Information and mitigating damages.

134. As a result of the Data Breach, Plaintiff and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, paying for credit monitoring and identity theft prevention services that, in some cases, were not offered to them by Defendant, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

135. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

136. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

137. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

SECOND CAUSE OF ACTION
VIOLATIONS OF THE SOUTH CAROLINA CODE OF LAWS, S.C. STAT., TIT. 39, CH. 5 §§ 10, *ET SEQ.*
(On Behalf of Plaintiff and the South Carolina Subclass)

138. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

139. Plaintiff brings this claim on behalf of himself and the South Carolina Subclass.

140. Defendant is a "person," as defined by S.C. Stat. § 39-5-10(a).

141. Defendant offers, sells, and distribute goods, services, and property, tangible or intangible, real, personal or mixed, and engage in trade and commerce that directly or indirectly affects the people of South Carolina. S.C. Stat. § 39-5-10(b).

142. Defendant, in the course of its business, engaged in unlawful practices in violation of S.C. Stat. § 39-5-20 (as guided by the interpretations given by the Federal Trade Commission and Federal Courts to Section 5(a)(1) of the FTC Act (15 U.S.C. 45(a)(1)), including unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

143. Defendant's unlawful, unfair, and deceptive practices include:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' Personal and Medical Information, which was a direct and proximate cause of the Data Breach;

b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous data incidents in the healthcare industry, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Personal and Medical Information, including duties imposed by the FTC Act and HIPAA;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' Personal and Medical Information, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Personal and Medical Information, including duties imposed by the FTC Act and HIPAA;

f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Personal and Medical Information; and

g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Personal and Medical Information, including duties imposed by the FTC Act and HIPAA.

144. Defendant's representations and omissions were material because they were likely to deceive reasonable patient consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their Personal and Medical Information.

145. Had Defendant disclosed to Plaintiff and Class members that its data security protocols were not secure and, thus, vulnerable to attack, Defendant would not have been able to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

146. The above unlawful practices and acts by Defendant was immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial and continuous injury to Plaintiff and Class members.

147. As a direct and proximate result of Defendant's unlawful practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including time and expenses related to monitoring their credit and medical accounts; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal and Medical Information.

148. Plaintiff and South Carolina Subclass members therefore seek all monetary and non-monetary relief allowed by law under S.C. Stat. § 39-5-10 et seq. for Defendant's violations alleged herein, including actual damages, civil penalties, and attorneys' fees and costs.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class or, alternatively, Plaintiff and the South Carolina Subclass)

149. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

150. Plaintiff and the Class bring this claim in the alternative to all other claims and remedies at law.

151. Plaintiff and Class members indirectly conferred a monetary benefit upon Defendant in the form of monetary payments to obtain medical services from providers who utilize Defendant's suite of medical practice management software.

152. Defendant collected, maintained, and stored the Personal and Medical Information of Plaintiff and Class members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and Class members.

153. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with Plaintiff and the Class members, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on HIPAA compliance and reasonable data privacy and security measures to secure Plaintiff's and Class members' Personal and Medical Information.

154. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Personal and Medical Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class members.

155. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiff and Class members suffered and continue to suffer actual damages in (i) the amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's Personal and Medical Information, (ii) time and expenses mitigating harms, (iii) diminished value of Personal and Medical Information, (iv) loss of privacy, and (v) an increased risk of future identity theft.

156. Defendant, upon information and belief, have therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff' and Class members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of their breach.

157. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

FOURTH CAUSE OF ACTION
INTRUSION UPON SECLUSION/INVASION OF PRIVACY (ELECTRONIC INTRUSION)
(On Behalf of Plaintiff and the Class or, alternatively, Plaintiff and the South Carolina Subclass)

158. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

159. Plaintiff and Class members maintain a privacy interest in their Personal and Medical Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

160. Plaintiff and Class members' Personal and Medical Information was contained, stored, and managed electronically in QRS's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class members' identities, unique identification numbers, medical histories, and financial records that were only shared with QRS for the limited purpose of obtaining and paying for healthcare, medical goods and services.

161. Additionally, Plaintiff's and Class members' Personal and Medical Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Personal and Medica Information for fraud, identity theft, and other crimes without their knowledge and consent.

162. QRS's disclosure of Plaintiff's and Class members' Personal and Medical Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Personal and Medical Information is offensive to a reasonable person. QRS's disclosure of Plaintiff's and Class members' Personal and Medical Information to unauthorized

third parties permitted the physical and electronic intrusion into Plaintiff's and Class members' private quarters where their Personal and Medical Information was stored and disclosed private facts about their health into the public domain.

163. Plaintiff and Class members have been damaged by QRS's conduct, by incurring the harms and injuries arising from the Data Breach now and in the future.

FIFTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class or, alternatively, Plaintiff and the South Carolina Subclass)

164. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

165. When Plaintiff and the Class members provided their Personal and Medical Information to Defendant when seeking medical services, they entered into implied contracts in which Defendant agreed to comply with their statutory and common law duties to protect Plaintiff's and Class members' Personal and Medical Information and to timely notify them in the event of a data breach.

166. Defendant required patients to provide Personal and Medical Information in order to receive medical services from its affiliate doctors and clinicians.

167. Defendant affirmatively represented that it collected and stored the Personal and Medical Information of Plaintiff and the members of the Class in compliance with HIPAA and other statutory and common law duties, and using reasonable, industry standard means.

168. Based on the implicit understanding and also on Defendant's representations (as described above), Plaintiff and the Class accepted Defendant's offers and provided Defendant with their Personal and Medical Information.

169. Plaintiff and Class members would not have provided their Personal and Medical Information to Defendant had they known that Defendant would not safeguard their Personal and Medical Information as promised or provide timely notice of a data breach.

170. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

171. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' Personal and Medical Information and failing to provide them with timely and accurate notice of the Data Breach.

172. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendant's breach of the implied contract with Plaintiff and Class members.

SIXTH CAUSE OF ACTION
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiff and the Class or, alternatively, Plaintiff and the South Carolina Subclass)

173. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

174. As described above, Defendant made promises and representations to Plaintiff and the Class that they would comply with HIPAA and other applicable laws and industry best practices.

175. These promises and representations became a part of the contract between Defendant and Plaintiff and the Class.

176. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

177. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations, and when it engaged in unlawful practices under HIPAA. These acts and omissions included: representing that it would maintain adequate data privacy and security practices and procedures to safeguard the Personal and Medical Information from unauthorized disclosures, releases, data breaches, and theft; omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's Personal and Medical Information; and failing to disclose to the Class at the time they provided their Personal and Medical Information to them that Defendant's data security systems and protocols, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

178. Plaintiff and Class members did all or substantially all of the significant things that the contract required them to do.

179. Likewise, all conditions required for Defendant's performance were met.

180. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

181. Plaintiff and Class Members have been harmed by Defendant's breach of this implied covenant in the many ways described above, including overpayment for services, the purchase of identity theft monitoring services not provided by Defendant, imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their Personal and Medical Information, and the attendant long-term expenses of attempting to mitigate and insure against these risks.

182. Defendant is liable for this breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

183. Plaintiff and Class members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

SEVENTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class or, alternatively, Plaintiff and the South Carolina Subclass)

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

185. As previously alleged, Plaintiff and members of the Class are entered into contracts with Defendant, which contracts required Defendant to provide adequate security for the Personal and Medical Information they collected from Plaintiff and the Class.

186. Defendant owed and still owes a duty of care to Plaintiff and Class members that require them to adequately secure Plaintiff's and Class members' Personal and Medical Information.

187. Defendant still possess the Personal and Medical Information of Plaintiff and the Class members.

188. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class members.

189. Since the Data Breach, Defendant has not yet announced any changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Data Breach to occur and go undetected for months and, thereby, prevent further attacks.

190. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the

Personal and Medical Information in Defendant's possession is even more vulnerable to cyberattack.

191. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their Personal and Medical Information and Defendant's failure to address the security failings that lead to such exposure.

192. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

193. Plaintiff and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

b) Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c) Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d) Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e) Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f) Ordering that Defendant conduct regular database scanning and security checks; and

g) Ordering that Defendant routinely and continually conduct 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, Plaintiff and the Class pray for judgment against Defendant as follows:

a) An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b) A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c) An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d) An order requiring Defendant pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e) A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f) An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: December 29, 2021

Respectfully submitted,

John Spragens, TN BPR No. 31445
SPRAGENS LAW PLC
311 22nd Ave. N.
Nashville, TN 37203
T: (615) 983-8900
F: (615) 682-8533
john@spragenslaw.com

*William B. Federman, OBA #2853
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com

Counsel for Plaintiff and the Putative Classes
**Pro Hac Vice Application Forthcoming*